



U.S. Department of Justice

*Executive Office for United States Attorneys
Freedom of Information Act & Privacy Act Staff*

*Bicentennial Building
600 E Street, NW, Suite 7300
Washington, DC 20530*

*(202) 252-6020
(202) 252-6047 Fax*

May 12, 2017

John Greenwald, Jr.
The Black Vault



john@greenwald.com

Re: Request Number: EOUSA-2017-001076

Date of Receipt: April 5, 2017

Subject of Request: Petraeus Investigation – Records Pertaining to Civil Action No. 16-cv-00514

Dear John Greenwald, Jr.,

Your Freedom of Information Act/Privacy Act request for records released in the above-referenced action has been processed. This letter constitutes a reply from the Executive Office for United States Attorneys, the official record-keeper for all records located in this office and the various United States Attorneys' Office.

To provide you with the greatest degree of access authorized by the Freedom of Information Act and the Privacy Act, we have considered your request in light of the provisions of both statutes.

The records you seek are located in a Privacy Act system of records that, in accordance with regulations promulgated by the Attorney General, is exempt from the access provisions of the Privacy Act. 28 CFR § 16.81. We are making available to you documents that have been released in a previous FOIA request.

The exemption(s) cited for withholding records or portions of records are marked below. An enclosure to this letter explains the exemptions in more detail.

List of Exemptions:

b5
b6
b7C

For your convenience, we are also providing you with a direct link to the location of the recently unsealed search warrants located on the U.S. Attorney for the Western District of North

Carolina's website. The link to the website is: <http://www.ncwd.uscourts.gov/news/documents-released-general-petraeus>.

This is the final action on this above-numbered request. If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, DC 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following website: <https://foiaonline.regulations.gov/foia/action/public/home>. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

You may contact our FOIA Public Liaison at the telephone number listed above for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Enclosure(s)

Sincerely,



Kevin Krebs
Assistant Director

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

JUN - 2 2016

IN THE MATTER OF THE SEARCH OF)
THE PREMISES LOCATED AT)
[ADDRESS REDACTED],)
[ADDRESS REDACTED])

Case No. 1:13sw273

LIMITED UNSEALING ORDER

Upon motion of the United States of America, it appearing that on April 4, 2013, the Court issued a residential search warrant in the above-captioned case and placed under seal the warrant, the application for the warrant, and the affidavit in support of the application for the warrant; it further appearing that the government now seeks to unseal said documents, subject to redactions of personal identifying information, pursuant to Local Criminal Rule 49(B) of this Court (the search warrant materials, as redacted by the government, are attached hereto); it further appearing that the government wants to first provide counsel for the individual whose residence was the subject of the search the limited opportunity to review said documents (as redacted by the government), in order for counsel to determine whether he wishes to file an opposition to the unsealing; accordingly, it is hereby

ORDERED that the search warrant, application for search warrant, and affidavit in support of the application for the search warrant (as redacted by the government) are unsealed for a period of five (5) days for the limited purpose of having the government provide said documents to counsel for the individual whose residence was the subject of the search, in order for counsel to determine whether he wishes to file an opposition to the unsealing; it is further

ORDERED that the search warrant, application for search warrant, and affidavit in

support of the application for the search warrant, as redacted by the government, will be automatically unsealed five (5) days from the date of this Order, or as further ordered by the Court if counsel for the individual whose residence was the subject of the search files an opposition before the expiration of that five- (5) day period.

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

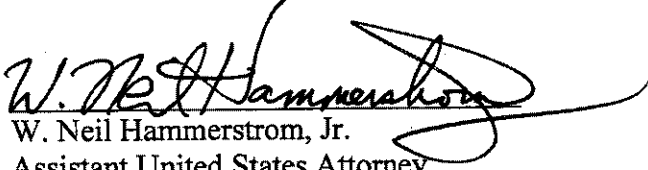

Theresa Carroll Buchanan
United States Magistrate Judge

Date: 6/2/16
At Alexandria, Virginia

WE ASK FOR THIS:

Dana J. Boente
United States Attorney

By:


W. Neil Hammerstrom, Jr.
Assistant United States Attorney

COPY**UNITED STATES DISTRICT COURT**for the
Eastern District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)THE PREMISES LOCATED AT
[REDACTED]

Case No. 1:13sw

273

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia
(Identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or beforeApril 18, 2013

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Ivan D. Davis

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.Date and time issued: 4 Apr 13 @ 1535 hrs[Signature]
Ivan D. Davis Judge's signature
United States Magistrate JudgeCity and state: Alexandria, Virginia

The Honorable Ivan D. Davis

Printed name and title

ATTACHMENT A

Property To Be Searched

This warrant applies to a single family home owned by [REDACTED], located at [REDACTED]
[REDACTED]. This property is further described as a two-story colonial house with [REDACTED]. The house has two floors and a basement. The residence is a single family detached home located on a [REDACTED] property. The home is approximately [REDACTED]
[REDACTED]. The number "[REDACTED]" appears above the main entrance door. The driveway is located to the left side of the main entrance as viewed from [REDACTED]. The premises is located on [REDACTED]
[REDACTED]

ATTACHMENT B

Particular Things To Be Seized

All records, information, documents, and items on the premises that relate to violations of: (a) Title 18, United States Code, Section 1924; (b) Title 18, United States Code, Section 793(e); and (c) Title 18, United States Code, Section 371, including:

1. All handwritten notes, documents, photographs or other instruments related to U.S. government operations;
 2. All records or information related to any communications between PETRAEUS and [REDACTED];
 3. All records or information related to any communications between PETRAEUS and any other person or entity concerning classified and/or national defense information from December 2008 to the present;
 4. All records or information related to any classified and/or national defense information from December 2008 to the present;
 5. All records or information related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED] from December 2008 to the present;
 6. All records or information related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information from December 2008 to the present;
 7. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;
-

8. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;
9. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS; and
10. Any information recording PETRAEUS's schedule or travel from December 2008 to the present.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

1. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. Evidence of the lack of such malicious software;
4. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

5. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
6. Evidence of the times the COMPUTER was used;
7. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
8. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
9. Records of or information about Internet Protocol addresses used by the COMPUTER;
10. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
11. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES DISTRICT COURT

for the
Eastern District of VirginiaFILED
APR - 4 2013UNDER SEAL
DISTRICT COURT
ALEXANDRIA, VIRGINIAIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)THE PREMISES LOCATED AT
[REDACTED]

Case No. 1:13sw

273

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 USC 1924; 18 USC 793(e); 18 USC 371 Unlawful removal and retention of classified documents; unlawful possession and communication of national defense information; conspiracy

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

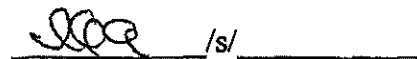


Applicant's signature

Diane M. Wehner, Special Agent, FBI

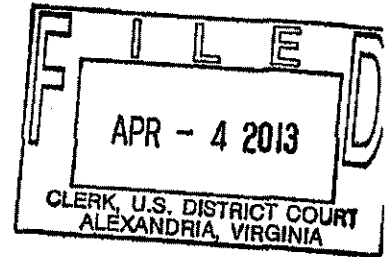
Printed name and title

Sworn to before me and signed in my presence.

Date: 04/04/2013City and state: Alexandria, Virginia
 /s/
Ivan D. Davis
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF)
THE PREMISES LOCATED AT)
[REDACTED],)
[REDACTED])

UNDER SEAL

Case No. 1:13sw

273

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, DIANE M. WEHNER, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search the residence of DAVID PETRAEUS, residing at [REDACTED]. The premises to be searched and items to be seized are more fully described in Attachments A and B.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for approximately seven years. I have investigated matters involving complex financial fraud, public corruption, and counterterrorism. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by individuals attempting to conceal their illegal behavior. I have also received specialized training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient

probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.
5. For the reasons set forth below, there is probable cause to believe that the PETRAEUS residence at [REDACTED] (and described in detail in Attachment A) contains evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful communication and/or retention of classified information.
6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.
9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."

10. E.O. 13526 also provides that certain senior U.S. officials are authorized to establish "special access programs" upon a finding that "the vulnerability of, or threat to, specific information is exceptional" and "the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure." Within the U.S. Intelligence Community, the Director of National Intelligence is authorized to establish special access programs for intelligence sources, methods, and activities. Such intelligence programs are called "Sensitive Compartmented Information Programs" or SCI Programs.
11. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

12. PETRAEUS is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about July 4, 2010 to July 18, 2011, PETRAEUS served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, PETRAEUS served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, PETRAEUS held a United States government security clearance allowing him access to classified United States government information. According to a Department of Defense (DOD) official, to obtain that clearance, PETRAEUS was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled

to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

13. [REDACTED] is a researcher and author of a biography of PETRAEUS, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. According to a DOD official, to obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
14. In 2012, [REDACTED] was the subject of an FBI Tampa Division (FBI Tampa) computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1. This complaint alleged the receipt of threatening and harassing emails from an unknown individual. Witness 1 claimed to have friendships with several high-ranking public and military officials.
15. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of PETRAEUS, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters notified PETRAEUS's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that PETRAEUS personally requested

that Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that PETRAEUS believed the alleged cyber stalker possessed information which could "embarrass" PETRAEUS and other public officials. Ultimately the FBI determined, based upon the investigation, that [REDACTED] was the individual who had sent the emails to Witness 1.

16. On September 24, 2012 as part of the FBI Tampa investigation, [REDACTED] consented to a search of two laptops and two external hard drives belonging to her. A review of the digital media contained on these devices revealed over 100 items which were identified by Charlotte Computer Analysis Response Team (CART) Forensic Examiners as potentially containing classified information, up to the Secret level.
17. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with [REDACTED]. He denied providing any classified documents to [REDACTED] or having any arrangement to provide her with classified information. PETRAEUS stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.
18. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her

time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from PETRAEUS.

19. During interviews conducted of [REDACTED] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of pre-paid cellular telephones and email accounts using non-attributable names. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if all the accounts were identified because both [REDACTED] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [REDACTED] September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

20. On November 12, 2012, Agents from the Charlotte and Tampa Divisions of the FBI participated in a consensual search of [REDACTED] residence in Charlotte, North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital

media as well as four boxes and one folder of documents. On this same date,

██████████ administrative assistant voluntarily provided the FBI with digital media as well as one box of documents which she maintained in her home in relation to her employment with ██████████. A review of the seized materials has identified to date hundreds of potentially classified documents, including more than 300 marked Secret, on digital images maintained on various pieces of electronic media.

21. Of the potentially classified documents reviewed to date, the majority relate to U.S.

military operations conducted in Afghanistan. ██████████ traveled into and out of Afghanistan several times between September 2010 and July 2011 to conduct research for a biography on PETRAEUS. During this time, PETRAEUS was serving as the International Security Assistance Force (ISAF) Commander.

22. ██████████ paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting ██████████ access to classified information for the purpose of writing his biography. For example, in an email dated January 16, 2011, which Petraeus marked as CONFIDENTIAL and sent to multiple members of the military, he instructed a member of his staff to "PLS PRINT FOR ██████████ ON AN OFF THE RECORD BASIS." Travel documents show that ██████████ was in Afghanistan at this time.

A. Communications Regarding Potential Mishandling of Classified Information

23. On May 12, 2011, ██████████, using email account ██████████, sent an email to PETRAEUS at email account ██████████. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training,

experience, and information reviewed to date in this investigation, your affiant believes the email related to a document or series of documents provided by PETRAEUS to [REDACTED] which contained classified information.

24. Between July 13, 2011 and July 15, 2011, [REDACTED] and a U.S. Army Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED], emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED] on July 15, 2011, he advised he was working on the storyboards and asked her for "a good SIPR number."¹ Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) PETRAEUS at email account [REDACTED] [REDACTED] response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel likely reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

25. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED], and PETRAEUS, using email address [REDACTED]

¹ SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

[REDACTED], discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which PETRAEUS addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing PETRAEUS's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG." Based on information provided by DOD, your affiant has learned that for a part of 2011 PETRAEUS was provided base housing at Fort Myer in Arlington County, Virginia. According to DOD records, PETRAEUS was assigned to residential quarters on Lee Avenue on Fort Myer between March 1, 2011 and August 10, 2011. PETRAEUS's reference to "unpack[ing] at the house in late July/Aug," probably refers to his private residence at [REDACTED], as he was about to retire from the U.S. Army when he wrote that email and it is unlikely that he would unpack items at base housing he was to vacate in a very short time.² When PETRAEUS vacated the residential quarters on Fort Myer, the Physical Security Manager personally cleared the quarters and found no items left behind. The clearing of the quarters included a search of the attic and basement. According to the Physical Security Manager, if PETRAEUS was traveling, there were specified storage rooms

² The basement of PETRAEUS's residence at [REDACTED] contained a Sensitive Compartmented Information Facility (SCIF) installed by the Central Intelligence Agency. This SCIF was approved for the storage of Top Secret/SCI materials and was given final certification on August 10, 2011. It was closed and de-accredited on January 3, 2013 and physically removed by February 13, 2013.

available at the Military Police station on base where PETRAEUS could leave classified material. After PETRAEUS vacated the residential quarters, the only items related to PETRAEUS remaining at the storage facility at the Military Police station were pieces of CENTCOM equipment, which were subsequently retrieved by CENTCOM personnel.

26. In response to PETRAEUS's email about the items being in boxes that he will unpack in July or August, [REDACTED] wrote: "Thanks for your willingness to get out the boxes! [REDACTED], the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there."³ In response PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER." Your affiant believes that, based on the timing of this email, PETRAEUS's statement that the files are "at home" refers to the quarters on Fort Myer.⁴

27. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address [REDACTED], and [REDACTED], using email address [REDACTED], exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED]. PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of

³ NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

⁴ According to records provided by the Department of Defense, PETRAEUS and other senior Army officials were permitted to store and access up to Secret-level data in on-post residential quarters at Fort Myer. This special approval was set forth in a March 15, 2010 memorandum and authorized such storage and access during the entire period in which PETRAEUS was assigned to residential quarters on Fort Myer in 2011.

the documents. [REDACTED] expressed her excitement about PETRAEUS's willingness to share the files writing: "[I]'ll protect them. And I'll protect you." PETRAEUS later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."⁵ PETRAEUS continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!**" (emphasis added).

28. Your affiant believes that PETRAEUS's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified. Your affiant also believes that, based on the timing of this email, PETRAEUS's statement that the files are "at home" refers to the residential quarters on Fort Myer.

B. Audio Recordings Indicating Potential Mishandling of Classified Information

29. PETRAEUS, in his capacity as ISAF Commander, maintained a digital recorder and may have used the recorder to capture select conversations. Your affiant has identified at least five images on the internet which show PETRAEUS with a recorder. One image shows PETRAEUS in military uniform, apparently in Afghanistan, another is a photograph from _____

[REDACTED] Facebook account showing PETRAEUS and [REDACTED] sitting

⁵ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). PETRAEUS was the former commander of MNF-I.

together in an office, believed to be PETRAEUS's office in Afghanistan. Your affiant has reviewed audio files recovered from [REDACTED] digital media and identified recorded conversations in which [REDACTED] is not heard on the recording and is not believed to have been present. Based upon the content of these recordings, your affiant believes the recorded conversations were originated by PETRAEUS. Your affiant has reviewed publicly available video and audio voice files of PETRAEUS and believes that the above-referenced recordings do include the voice of PETRAEUS. Investigators have not yet recovered any digital recorders from [REDACTED] or PETRAEUS.

30. In an audio file located on a computer received from [REDACTED] administrative assistant, there is a recording of an interview conducted by [REDACTED] during the course of her research on PETRAEUS. This recording is approximately twenty-four minutes, and based on the content of the audio, seems to have been recorded in the August 2011 timeframe. During the recorded conversation, [REDACTED] informed an unknown individual she was interviewing that she would be traveling to Washington, D.C. a lot that month to meet with PETRAEUS and would go through boxes in "his attic." As noted above, although [REDACTED] is not specific as to which PETRAEUS home she is referring, your affiant believes that based on the timeframe of the recording, it is likely that [REDACTED] was referring to the attic in PETRAEUS's residence at Fort Myer.

31. In an audio file located on a hard drive seized from [REDACTED] residence on November 12, 2012, there is a recorded conversation between PETRAEUS and, inter alia, Washington Post reporters, which, based on the information and belief of your affiant, occurred in or about March 2011. In the conversation, PETRAEUS stated, "[I]

would really love to be on background as a senior military officer.” Later in the recording, PETRAEUS discusses sensitive military campaigns and operations, some of which, on the basis of a preliminary review by another government agency designated to assist in this investigation, is believed to contain classified information, including information at the Top Secret level.

32. In an audio file located on electronic evidence seized from [REDACTED] residence on November 12, 2012, there is a recorded conversation between PETRAEUS, a reporter, and at least one other individual. During the conversation, PETRAEUS requested that information he provided be attributed to a “defense official familiar with PETRAEUS’s activities.” PETRAEUS was concerned about the sensitivity of the information he was providing, and wanted to ensure the information was not attributed to him because it would come out after he was confirmed as Director of the CIA. PETRAEUS then discussed with the reporter information that, on the basis of a preliminary review by another government agency designated to assist in this investigation, is believed to be classified, including information at the Top Secret level.

C. Additional Evidence of Potential Mishandling of Classified Information

33. A review of [REDACTED] digital media has identified photographs of at least two black books which appear to be the daily event and calendar books used by PETRAEUS to memorialize significant events during his military assignments. Investigators have reviewed the metadata from some of the digital media obtained consensually from [REDACTED] and have determined that from on or about August 29, 2011 to on or about August 31, 2011, there were approximately one hundred and seventeen separate photographs taken of the contents of the black books. These photographs have been reviewed by your affiant in close coordination with other government agencies

designated to assist with this investigation. Based upon a preliminary review by another government agency designated to assist in this investigation, your affiant has reason to believe that at least five photographs contain classified information, including information up to the Top Secret level.

34. Additional review of embedded metadata, including date and time stamps, allowed investigators to identify specific photographs from [REDACTED] digital media. On August 29, 2011, at 9:47 a.m., two photographs were taken of the front cover of a black book which had PETRAEUS's personal business card taped to the front cover. The business card identified PETRAEUS as "General David H. Petraeus, Commander, International Security Assistance Force."
35. An 8.5 x 11 inch sized printed photograph was located during the consensual search of [REDACTED] residence on November 12, 2012. This photograph showed the content of a black book, specifically a page containing a daily calendar for December 3, 2010 on the left side of the notebook and handwritten notes on the right side of the notebook. The written entry on the top line read, "[REDACTED] C-N Community of Interest." The calendar in the photograph reflected a "CN Briefing" between 1:45 p.m. and 2:30 p.m. on December 3, 2010. Your affiant believes that the written note for [REDACTED] was added by PETRAEUS so as to provide [REDACTED] context in reading that day's calendar entry. An initial review of the calendar and notes on this specific image revealed a reference to military units and potential needs for these units.
36. Open source information includes a photograph depicting PETRAEUS with a black book. See www.thedailybeast.com/newsweek/2011/07/17/general-david-petraeus-on-leaving-afghanistan-and-going-to-cia.html. Based on my review, I believe that the black book

depicted in the photographs described in paragraph 34 above is the same black book depicted in a photograph of PETRAEUS in the news article on the above-mentioned website. The photograph shows PETRAEUS, while in Afghanistan, standing with then-Secretary of Defense Leon Panetta and General John Allen. This photograph, dated July 9, 2011, reportedly captured PETRAEUS while he was ending his command in Afghanistan. On the table next to PETRAEUS in the same photograph, is a similarly-sized black book with a business card taped to the front. The format of the business card, its position on the book, the manner in which it is taped to the book, and its general characteristics are very similar to the photographs of the front cover of a black book located on [REDACTED] digital media.

37. In an email dated June 26, 2011, an Army historian previously assigned to ISAF replied to an email from PETRAEUS in which PETRAEUS discussed [REDACTED] research efforts. In the body of the Army historian's response, the historian wrote, "I [am] happy to receive [REDACTED] research effort and will add it to the collection. It is still my understanding that your 'black books' and other sensitive items are off limits. She can look at the other documents such as update briefs, info papers, photos, and other reference materials, but not the sensitive ones. Am I correct on that rule?"
38. In an audio file located on a laptop computer seized from [REDACTED], there is a recorded conversation between [REDACTED] and PETRAEUS, which is approximately twenty-five minutes long, and, based on the content of the entire recording, seems to have been recorded in late July/early August of 2011. In the recording, [REDACTED] asked PETRAEUS about the location of the "black books." PETRAEUS responded that the black books are "in a rucksack up there somewhere." PETRAEUS further stated the

black books, "are highly classified, some of them, they don't have it on it, but I mean there's code word stuff in there..." Your affiant believes that when PETRAEUS stated that "there's code word stuff in there," it is possible that he was indicating that there was special access program information contained in the black books. Moreover, your affiant believes PETRAEUS's reference to "they don't have it on it" indicates that the black books do not have the proper classification markings on them. Just as in paragraphs 28 and 30 above, the statement regarding the location of the materials likely referred to PETRAEUS's former residence at Fort Myer. Photographs of the contents of these black books were found during the review of digital and physical evidence recovered during the consensual search of [REDACTED] house.

39. Additional review of [REDACTED] digital media also revealed multiple photographs taken between August 16, 2011 and August 17, 2011. On review of the photographs and the embedded metadata, investigators have determined the following:

- a. On August 16, 2011 at 11:04 p.m., a photograph was taken of at least three medium-sized cardboard boxes sitting on a bed. In the photograph, the boxes are open, and although the contents are unknown, there appear to be some file folders visible inside the boxes. Sitting on the bed next to the boxes is a black laptop computer which is open and powered on, though the screen image is difficult to discern.
- b. On August 16, 2011 at 11:04 p.m., a second photograph from a different angle was taken of the same boxes referenced above. The boxes are open, and one box has the letters "Petrae" written in black and clearly visible on the side. Your

affiant believes this writing spelled out "Petraeus," as the "us" in "Petraeus" was partially obscured.

- c. On August 17, 2011 at 9:23 a.m., [REDACTED] is observed in a photograph which she took of herself in a mirror. In the photograph, [REDACTED] is posing next to the same bed mentioned in paragraphs 39a and 39b above. In this photograph, what appear to be two of the same boxes are visible on the bed. The boxes are open, though the contents of the boxes cannot be clearly discerned.

40. The boxes and black books photographed by [REDACTED], and believed to belong to PETRAEUS, were not recovered during the consensual search conducted at [REDACTED] residence on November 12, 2012, nor were they recovered when the Sensitive Compartmented Information Facility in PETRAEUS's residence was cleared by CIA personnel after PETRAEUS's resignation as Director in November 2012.

41. Based upon PETRAEUS's description of the various items your affiant believes PETRAEUS had stored in the residential quarters at Fort Myer, including both the black books described in paragraph 38 above as well as the files and boxes discussed in paragraphs 25-27 above, it appears that that he had kept some of these materials for nearly a decade, and thus through various geographical moves in the military. Your affiant believes that these are items PETRAEUS values, and it is therefore likely he would have taken them with him when he was required to vacate the residential quarters at Fort Myer and moved to his private residence at [REDACTED]
- [REDACTED]

D. Continuing Communications Between PETRAEUS and [REDACTED]

42. [REDACTED] and PETRAEUS are believed to have had multiple telephonic contacts after being made aware of FBI Tampa's computer intrusion investigation. Your affiant asserts:

- a. PETRAEUS's CIA security detail was notified of the FBI investigation on June 22, 2012. In an interview with FBI Tampa on October 26, 2012, PETRAEUS acknowledged that: (1) he was briefed by the security detail concerning the FBI investigation, and (2) he called [REDACTED] on June 23, 2012 regarding the emails received by Witness 1.
- b. Over the weekend of August 11, 2012 and August 12, 2012, PETRAEUS spoke to Witness 1. In evidence reviewed by FBI Charlotte, a telephone number attributed to [REDACTED] called a telephone number attributed to PETRAEUS on August 11, 2012.
- c. [REDACTED] was interviewed by FBI Tampa on September 24, 25, and 26, 2012. A telephone number attributed to [REDACTED] called a telephone number attributed to PETRAEUS on three occasions on September 25, 2012.
- d. [REDACTED] was in contact with FBI Tampa on October 1 and 2, 2012. These contacts ultimately resulted in a telephone interview conducted on October 3, 2012. In evidence reviewed by FBI Charlotte, on October 2, 2012, there were six calls between telephone numbers attributed to [REDACTED] and PETRAEUS. One of these calls connected, resulting in an approximately fifteen-minute-long conversation.

- e. During the October 26, 2012 interview of PETRAEUS by FBI Tampa, he stated that, while coming back from a trip to the Far East earlier in the month, he called [REDACTED], who told him about her interview with the FBI. Evidence indicated that a telephone number attributed to PETRAEUS called a telephone number attributed to [REDACTED] on October 16, 2012.
 - f. Following FBI Tampa's interview of PETRAEUS on October 26, 2012, a telephone number attributed to [REDACTED] called a telephone number attributed to PETRAEUS on four occasions on October 27, 2012, on three occasions on October 28, 2012, and on two occasions on October 29, 2012.
 - g. On November 2, 2012, [REDACTED] was again interviewed by FBI Tampa. [REDACTED] stated that she and PETRAEUS had talked candidly since each of their interviews with the FBI.
 - h. On November 9, 2012, [REDACTED] contacted FBI Tampa telephonically from telephone number [REDACTED]. She advised she received a telephone call from PETRAEUS earlier that day advising her of his resignation. In evidence reviewed by FBI Charlotte, telephone number [REDACTED] called a telephone number attributed to PETRAEUS on November 9, 2012.
43. The foregoing telephone communications identified in this affidavit only include calls made or received from one government phone attributed to PETRAEUS. As detailed above, PETRAEUS and [REDACTED] have previously been in regular contact through email, and communicated about the provision of classified information to [REDACTED]. Moreover, [REDACTED] and PETRAEUS have admitted that they established covert communications systems using pre-paid cellular telephones and non-

attributable email accounts. To date, the pre-paid telephone numbers used by PETRAEUS and [REDACTED] have not been identified.

LOCATION TO BE SEARCHED

44. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for PETRAEUS's residence, as more fully described in Attachment A to this affidavit, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.
45. On April 2, 2013, a search of the CLEAR public source database for the address [REDACTED] [REDACTED], revealed the residence was owned by [REDACTED] and that it was purchased on [REDACTED]. Consistent with his obligations as a government employee, PETRAEUS filed a 2011 financial disclosure form with the United States government, listing his home address as [REDACTED] [REDACTED]. The form stated that PETRAEUS purchased the residence in [REDACTED] for a purchase price of [REDACTED] and also stated that PETRAEUS and his wife are trustees of [REDACTED] the company that owns the residence at [REDACTED] [REDACTED]. Given the information noted in the financial disclosure, as well as information provided by the CIA, your affiant believes that PETRAEUS's current residence is [REDACTED].

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

46. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
47. The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
48. As described above and in Attachment B, this application seeks permission to search for records that might be found on the premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).
49. I submit that if a computer or storage medium is found on the premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:
- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

50. Forensic evidence: As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of their use, who used them, and

when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

51. Necessity of seizing or copying entire computers or storage media: In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises

could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

52. Nature of examination: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. Searches and seizures of evidence from computers commonly requires agents to download or copy information from the computer and components, and to seize the computer to be processed later by a qualified computer expert in a laboratory or other controlled environment. Searching computer systems for evidence is an exacting

scientific procedure that is designed to protect the integrity of the evidence and to recover hidden, erased, deleted, compressed, password-protected, or encrypted files. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

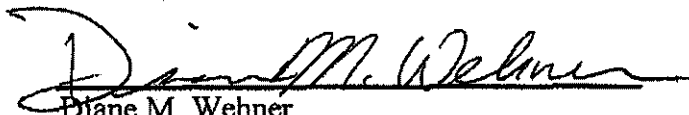
53. Because more than one person uses the premises as a residence, it is possible that the premises will contain storage media that are predominantly used, and perhaps owned, by a person who is not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

54. Based upon the foregoing, your affiant submits that sufficient probable cause exists for the issuance of a warrant to search [REDACTED], as further described in Attachments A and B; and that the described premises contains evidence of a crime relating to: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.


REQUEST FOR SEALING

55. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.



Diane M. Wehner
Special Agent
FBI Charlotte Division

Sworn to and subscribed before me
this 4th day of April, 2013.

 /s/ _____
Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

Property To Be Searched

This warrant applies to a single family home owned by [REDACTED], located at [REDACTED]

[REDACTED] This property is further described as a two-story colonial house [REDACTED]. The house has two floors and a basement. The residence is a single family detached home located on a [REDACTED] The home is approximately [REDACTED] [REDACTED] [REDACTED]. The number [REDACTED] appears above the main entrance door. The driveway is located to the left side of the main entrance as viewed from [REDACTED]. The premises is located on [REDACTED].

ATTACHMENT B

Particular Things To Be Seized

All records, information, documents, and items on the premises that relate to violations of: (a) Title 18, United States Code, Section 1924; (b) Title 18, United States Code, Section 793(e); and (c) Title 18, United States Code, Section 371, including:

1. All handwritten notes, documents, photographs or other instruments related to U.S. government operations;
2. All records or information related to any communications between PETRAEUS and [REDACTED];
3. All records or information related to any communications between PETRAEUS and any other person or entity concerning classified and/or national defense information from December 2008 to the present;
4. All records or information related to any classified and/or national defense information from December 2008 to the present;
5. All records or information related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED] from December 2008 to the present;
6. All records or information related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information from December 2008 to the present;
7. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

8. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;
9. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS; and
10. Any information recording PETRAEUS's schedule or travel from December 2008 to the present.

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

1. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. Evidence of the lack of such malicious software;
4. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

5. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
6. Evidence of the times the COMPUTER was used;
7. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
8. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
9. Records of or information about Internet Protocol addresses used by the COMPUTER;
10. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
11. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.



PDF Version

UNCLASSIFIED//FOUO

*Central Intelligence Agency
Inspector General*

REPORT OF INVESTIGATION



IMPROPER HANDLING OF CLASSIFIED INFORMATION BY JOHN M. DEUTCH (1998-0028-IG)

February 18, 2000

L. Britt Snider
Inspector General

Daniel S. Seikaly
Assistant Inspector General for Investigations

This Report contains information that is or may be subject to the protections of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, or that otherwise may implicate the privacy interests of various current or former federal employees and private citizens.

TABLE OF CONTENTS

INTRODUCTION

SUMMARY

BACKGROUND

PROCEDURES AND RESOURCES

QUESTIONS PRESENTED

CHRONOLOGY OF SIGNIFICANT EVENTS

FINDINGS

WHY WAS DEUTCH ISSUED GOVERNMENT COMPUTERS CONFIGURED FOR UNCLASSIFIED USE AND WERE HIS COMPUTER SYSTEMS APPROPRIATELY MARKED AS UNCLASSIFIED?

WHY WAS DEUTCH PERMITTED TO RETAIN GOVERNMENT COMPUTERS AFTER RESIGNING AS DCI?

WHAT INFORMATION WAS FOUND ON DEUTCH'S MAGNETIC MEDIA?

WHAT VULNERABILITIES MAY HAVE ALLOWED THE HOSTILE EXPLOITATION OF DEUTCH'S UNPROTECTED COMPUTER MEDIA?

COULD IT BE DETERMINED IF CLASSIFIED INFORMATION ON DEUTCH'S UNCLASSIFIED COMPUTER WAS COMPROMISED?

WHAT KNOWLEDGE DID DEUTCH HAVE CONCERNING VULNERABILITIES ASSOCIATED WITH COMPUTERS?

HAD DEUTCH PREVIOUSLY BEEN FOUND TO HAVE MISHANDLED CLASSIFIED INFORMATION?

WHAT LAWS, REGULATIONS, AGREEMENTS, AND POLICIES HAVE POTENTIAL APPLICATION?

HOW WAS A SIMILAR CASE HANDLED?

WHAT ACTIONS DID SENIOR AGENCY OFFICIALS TAKE IN HANDLING THE DEUTCH CASE?

SHOULD A CRIMES REPORT INITIALLY HAVE BEEN FILED ON DEUTCH IN THIS CASE?

SHOULD APPLICATION OF THE INDEPENDENT COUNSEL STATUTE HAVE BEEN CONSIDERED?

WERE SENIOR AGENCY OFFICIALS OBLIGATED TO NOTIFY THE CONGRESSIONAL OVERSIGHT COMMITTEES OR THE INTELLIGENCE OVERSIGHT BOARD OF THE PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD? WERE THESE ENTITIES NOTIFIED?

WHY WAS NO ADMINISTRATIVE SANCTION IMPOSED ON DEUTCH?

WHAT WAS OIG's INVOLVEMENT IN THIS CASE?

WHAT IS DEUTCH's CURRENT STATUS WITH THE CIA?

WHAT WAS THE DISPOSITION OF OIG's CRIMES REPORT TO THE DEPARTMENT OF JUSTICE?

CONCLUSIONS

RECOMMENDATIONS

*OFFICE OF INSPECTOR GENERAL
INVESTIGATIONS STAFF*

REPORT OF INVESTIGATION

**IMPROPER HANDLING OF CLASSIFIED INFORMATION BY
JOHN M. DEUTCH
(1998-0028-IG)**

February 18, 2000

This unclassified report has been prepared from the July 13, 1999 version of the classified Report of Investigation at the request of the Senate Select Committee on Intelligence. Information in this version is current as of the date of the original report. All classified information contained in the original Report of Investigation has been deleted.

INTRODUCTION

1. (U//FOUO) John M. Deutch held the position of Director of Central Intelligence (DCI) from May 10, 1995 until December 14, 1996. Several days after Deutch's official departure as DCI, classified material was discovered on Deutch's government-owned computer, located at his Bethesda, Maryland residence.
2. (U//FOUO) The computer had been designated for unclassified use only and was connected to a modem. This computer had been used to access [an Internet Service Provider (ISP)], the Internet, [Deutch's bank], and the Department of Defense (DoD). This report of investigation examines Deutch's improper handling of classified information during his tenure as DCI and how CIA addressed this matter.
3. (U//FOUO) Currently, Deutch is a professor at the Massachusetts Institute of Technology. He also has two, no-fee contracts with the CIA. The first is to provide consulting services to the current DCI and his senior managers; this contract went into effect on December 16, 1996, has been renewed twice, and will expire in December 1999. The second contract is for Deutch's appointment to serve on the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction (Proliferation Commission). Under the terms of the second contract, this appointment will continue until the termination of the Commission.

SUMMARY

4. (U//FOUO) The discovery of classified information on Deutch's unclassified computer on December 17, 1996 was immediately brought to the attention of senior Agency managers. In January

1997, the Office of Personnel Security (OPS), Special Investigations Branch (SIB), was asked to conduct a security investigation of this matter.¹ A technical exploitation team, consisting of personnel expert in data recovery, retrieved the data from Deutch's unclassified magnetic media and computers. The results of the inquiry were presented to CIA senior management in the spring and summer of 1997.

¹ (U//FOUO) OPS was established in 1994 and was subsumed as part of the new Center for CIA Security in 1998. The mission of OPS was to collect and analyze data on individuals employed by or affiliated with the Agency, for the purpose of determining initial and continued reliability and suitability for access to national security information. SIB conducts investigations primarily related to suitability and internal security concerns of the Agency. SIB often works with the OIG, handling initial investigations, and refers cases to the OIG and/or the proper law enforcement authority once criminal conduct is detected.

5. (U//FOUO) The Office of General Counsel (OGC) had been informed immediately of the discovery of classified information on Deutch's computer. Although such a discovery could be expected to generate a crimes report to the Department of Justice (DoJ), OGC determined such a report was not necessary in this case. No other actions, including notification of the Intelligence Oversight Committees of the Congress² or the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board, were taken until the Office of Inspector General (OIG) opened a formal investigation in March 1998. On March 19, 1998, OIG referred the matter to DoJ. On April 14, 1999, the Attorney General declined prosecution and suggested a review to determine Deutch's suitability for continued access to classified information.

² (U//FOUO) Congressional oversight is provided by the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on intelligence (HPSCI). The two appropriations committees -- the Senate Appropriations Committee, Subcommittee on Defense(SAC) and the House Appropriations Committee, National Security Subcommittee (HAC) -- also bear oversight responsibilities.

6. (U//FOUO) Deutch continuously processed classified information on government-owned desktop computers configured for unclassified use during his tenure as DCI. These unclassified computers were located in Deutch's Bethesda, Maryland and Belmont, Massachusetts residences,³ his offices in the Old Executive Office Building (OEOB), and at CIA Headquarters. Deutch also used an Agency-issued unclassified laptop computer to process classified information. All were connected to or contained modems that allowed external connectivity to computer networks such as the Internet. Such computers are vulnerable to attacks by unauthorized persons. CIA personnel retrieved [classified] information from Deutch's unclassified computers and magnetic media related to covert action, Top Secret communications intelligence and the National Reconnaissance Program budget.

³ (U//FOUO) Hereafter, the residences will be referred to as Maryland and Belmont.

7. (U//FOUO) The OIG investigation has established that Deutch was aware of prohibitions relating to the use of unclassified computers for processing classified information. He was further aware of specific vulnerabilities related to the use of unclassified computers that were connected to the Internet. Despite this knowledge, Deutch. processed a large volume of highly classified information on these unclassified computers, taking no steps to restrict unauthorized access to the information and thereby placing national security information at risk.

8. (U//FOUO) Furthermore, the OIG investigation noted anomalies in the way senior CIA officials responded to this matter. These anomalies include the failure to allow a formal interview of Deutch, and the absence of an appropriate process to review Deutch's suitability for continued access to classified information.

BACKGROUND

9. (U//FOUO) In 1998, during the course of an unrelated investigation, OIG became aware of additional circumstances surrounding an earlier allegation that in 1996 Deutch had mishandled classified information. According to the 1996 allegation, classified information was found on a computer configured for unclassified use at Deutch's Maryland residence. This computer had been used to connect to the Internet. Additionally, unsecured classified magnetic media was found in Deutch's study at the residence. Further investigation uncovered additional classified information on other Agency-owned unclassified computers issued to Deutch. In 1998, OIG learned that senior Agency officials were apprised of the results of the OPS investigation but did not take action to properly resolve this matter. The Inspector General initiated an independent investigation of Deutch's alleged mishandling of classified information and whether the matter was appropriately dealt with by senior Agency officials.

PROCEDURES AND RESOURCES

10. (U//FOUO) OIG assigned a Supervisory Investigator, five Special Investigators, a Research Assistant, and a Secretary to this investigation. The team of investigators interviewed more than 45 persons thought to possess knowledge pertinent to the investigation, including Deutch, DCI George Tenet, former CIA Executive Director Nora Slatkin, former CIA General Counsel Michael O'Neil, and [the] former FBI General Counsel. The team reviewed security files, memoranda for the record written contemporaneously with the events under investigation, data recovered from Deutch's unclassified magnetic media, Congressional testimony, and material related to cases involving other individuals who mishandled classified information. Pertinent information was also sought from the National Security Agency (NSA), the DoD, and an Internet service provider (ISP). In addition, the team reviewed applicable criminal statutes, Director of Central Intelligence Directives, and Agency rules and regulations.

QUESTIONS PRESENTED

11. (U//FOUO) This Report of Investigation addresses the following questions:

- Why was Deutch issued government computers configured for unclassified use and were his computer systems appropriately marked as unclassified?
- Why was Deutch permitted to retain government computers after resigning as DCI?
- What information was found on Deutch's magnetic media?
 - How was the classified material discovered?
 - What steps were taken to gather the material?
 - What steps were taken to recover information residing on Deutch's magnetic media?
 - What are some examples of the classified material that was found?
- What vulnerabilities may have allowed the hostile exploitation of Deutch's unprotected computer media?
 - What was- the electronic vulnerability of Deutch's magnetic media?
 - What was the physical vulnerability of Deutch's magnetic media?
- Could it be determined if classified information on Deutch's unclassified computer was compromised?
- What knowledge did Deutch have concerning vulnerabilities associated with computers?
 - What is Deutch's recollection?
 - What did Deutch learn at [an] operational briefing?
 - What was Deutch's Congressional testimony?
 - What are the personal recollections of DCI staff members?
- Had Deutch previously been found to have mishandled classified information?
- What laws, regulations, agreements, and policies have potential application?
- How was a similar case handled?

- What actions did senior Agency officials take in handling the Deutch case?
 - What actions were taken by senior Agency officials after learning of this matter?
 - How were the Maryland Personal Computer Memory Card International Association (PCMCIA) cards handled?
 - What was the course of the Special Investigations Branch's investigation of Deutch?
- Should a crimes report initially have been filed on Deutch in this case?
- Should application of the Independent Counsel statute have been considered?
- Were senior Agency officials obligated to notify the Congressional oversight committees or the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board? Were these entities notified?
- Why was no administrative sanction imposed on Deutch?
- What was OIG's involvement in this case?
 - When did OIG first learn of this incident?
 - Why did OIG wait until March 1998 to open an investigation?
 - What steps were taken by OIG after opening its investigation?
- What is Deutch's current status with the CIA?
- What was the disposition of OIG's crimes report to the Department of Justice?

(U//FOUO) CHRONOLOGY OF SIGNIFICANT EVENTS

1995

January 1 John Deutch establishes Internet access via an [ISP provider].

May 10 Deutch sworn in as DCI

June 15 Earliest classified document later recovered by technical exploitation team.

August 1 Deutch receives [a] briefing on computer attacks.

1996

December 5 Deutch requests that he be able to retain computers after he leaves office.

December 13 Deutch signs a no-fee consulting contract permitting him to retain government computers.

December 14 Deutch's last day as DCI.

December 17 Classified information found on Deutch's computer in Bethesda, Maryland. Slatkin and O'Neil notified. Slatkin notifies Tenet within a day. O'Neil informs Deutch of discovery.

December 23 Four PCMCIA cards retrieved from Deutch and given to O'Neil.

December 27 Hard drive from Deutch's Maryland computer retrieved.

December 28 Chief/DCI Administration informs IG Hitz of discovery at Deutch's residence.

December 30 Hard drives from residences given to O'Neil.

1997

January 6 OPS/SIB initiates investigation on Deutch. PDGC and the OPS Legal Advisor discuss issue of a crimes report.

January 9 O'Neil releases to DDA Calder and C/SIB the hard drives from the residences and two of six PCMCIA cards. O'Neil retains four

PCMCIA cards from the Maryland residence.

January 9 Memo from ADCI to D/OPS directing Deutch to keep clearances through December 1997.

January 13 Technical exploitation team begins the recovery process.

January 22 Technical exploitation team documents that two hard drives contain classified information and had Internet exposure after classified material placed on drives.

January 30 O'Neil speaks with FBI General Counsel and was reportedly told that FBI was not inclined to investigate.

February 3 O'Neil releases four remaining PCMCIA cards that are subsequently exploited.

February 21 C/SIB meets with OIG officials to discuss jurisdictional issues.

February 27 D/OPS, tasked to review all material on hard drives and PCMCIA cards.

March 11 D/OPS completes review of 17,000 pages of recovered items.

July 8 D/OPS's report to ADCI prepared for distribution. Included on distribution are Slatkin, O'Neil, and Richard Calder.

July 21 Slatkin is replaced as Executive Director.

July 30 PDGC reaffirms with OGC attorney that original disks and hard drives need to be destroyed to ensure protection of Deutch's privacy.

August 11 PDGC appointed Acting General Counsel and O'Neil goes on extended annual leave.

August 12 Technical exploitation team confirms selected magnetic media were destroyed per instruction of D/OPS.

September 8 Slatkin leaves CIA.

October 1 O'Neil retires from CIA.

November 24 DCI approves Deutch and other members of the Proliferation Commission for temporary staff-like access to CIA information and facilities without polygraph.

1998

February 6 OIG is made aware of additional details of the SIB investigation and subsequently opens a formal investigation.

March 19 IG forwards crimes report to DoJ.

May 8 IG letter to IOB concerning Deutch investigation.

June 2 DCI notifies oversight committees of investigation.

1999

April 14 Attorney General Reno declines prosecution and suggests a review of Deutch's security clearances.

FINDINGS

WHY WAS DEUTCH ISSUED GOVERNMENT COMPUTERS CONFIGURED FOR UNCLASSIFIED USE AND WERE HIS COMPUTER SYSTEMS APPROPRIATELY MARKED AS UNCLASSIFIED?

12. (U//FOUO) The then-Chief of the Information Services Management Staff (C/ISMS) for the DCI Area, recalled that prior to Deutch's confirmation as DCI, she was contacted by [Deutch's Executive Assistant] regarding computer requirements for Deutch. C/ISMS, who would subsequently interface with [the Executive Assistant] on a routine basis, learned that Deutch worked exclusively on Macintosh computers. An Information Security (Infosec) Officer assigned to ISMS recalled C/ISMS stating that [the Executive Assistant] instructed [her] to provide Internet service at the 7th floor Headquarters suite, OEOB, and Deutch's Maryland residence.

13. (U//FOUO) According to C/ISMS, Deutch's requirements, as imparted by [his Executive Assistant], were for Deutch to have not only access to the Internet, including electronic messaging, but access to CIA's classified computer network from Deutch's offices in CIA Headquarters, OEOB, and his Maryland residence. In addition, Deutch was to be issued an unclassified laptop with Internet capability for use when traveling.

14. (U//FOUO) A computer specialist, who had provided computer support to Deutch at the Office of the Secretary of Defense, confirmed that, at Deutch's request, he had been hired by CIA to establish the same level of computer support Deutch had received at the Pentagon. At CIA, the computer specialist provided regular and cose computer support to Deutch on an average of once a week. The computer specialist recalled [that Deutch's Executive Assistant] relayed that he and Deutch had discussed the issue of installing the classified computer at Deutch's Maryland residence, and Deutch either did not believe he needed or was not comfortable having the classified computer in his home.

15. (U//FOUO) [Deutch's Executive Assistant] also remembered discussions about locating a classified computer at Deutch's Maryland residence. [The Executive Assistant], however, could not recall with any certainty if the computer had in fact been installed. [The Executive Assistant] said that a classified system had been installed at his own residence. However, after using it once, he found its operation to be difficult and time consuming, and he had it removed from his residence. [The Executive Assistant's] experience with the deployed classified system may have influenced Deutch to decide he did not want one located at his Maryland residence. If so, [the Executive Assistant] would have informed the ISMS representative of Deutch's decision.

16. (U//FOUO) C/ISMS recalled [the Executive Assistant] telling her he was not sure Deutch required a classified computer system at Deutch's Maryland residence.

17. (U//FOUO) A Local Area Network (LAN) technician installed classified and unclassified Macintosh computers in Deutch's 7th floor Headquarters office and in Deutch's OEOB office. The technician also installed a computer configured for unclassified use at Deutch's Maryland residence. The technician stated that Deutch was also provided with an unclassified laptop that had an internal hard drive with modem and Internet access. The computer specialist installed an unclassified computer at Deutch's Belmont residence several months after Deutch was appointed DCI.

18. (U//FOUO) Personal Computer Memory Card International Association (PCMCIA) cards are magnetic media capable of storing large amounts of data. According to the computer specialist, Deutch's unclassified computers were equipped with PCMCIA card readers. The computer specialist said this configuration afforded Deutch the opportunity to write to the cards and back up information. One PCMCIA card would reside at all times in a reader that was attached to the unclassified computer, and the other PCMCIA card would be in Deutch's possession. The computer specialist stated that Deutch valued the ability to access, at several locations, data on which he was working.

C/ISMS stated that all the unclassified computers and PCMCIA cards provided for Deutch's use contained a green label indicating the equipment was for unclassified purposes. The LAN technician also stated that a concern was to label all of Deutch's automated data processing equipment and magnetic media, including monitors and PCMCIA cards, as either "unclassified" (green label) or "Top Secret" (purple label). The technician stated that his purpose was to make it perfectly clear to Deutch and anyone else using these systems, what was for classified and unclassified use.

19. (U//FOUO) The OIG has in its possession eight PCMCIA cards that had been used by Deutch. Seven of the eight cards were labeled unclassified; the eighth was not labeled. Four of the cards were from the Maryland residence. Three of the cards were from CIA Headquarters and one was from the OEOB. In addition, OIG received four Macintosh computers and one Macintosh laptop that were used by Deutch. The laptop and two of the computers were marked with green unclassified labels; the other two computers were marked with purple classified labels. One of the classified computers was determined to have come from Deutch's 7th floor Headquarters office; the other from his OEOB office.

WHY WAS DEUTCH PERMITTED TO RETAIN GOVERNMENT COMPUTERS AFTER RESIGNING AS DCI?

20. (U//FOUO) In a Memorandum for the Record (MFR) dated December 30, 1996, [the] then Chief DCI Administration (C/DCI Administration), noted that Deutch announced on December 5, 1996 that he would resign as DCI. That same day, according to C/DCI Administration's MFR, Deutch summoned [him] to his office. Deutch told [him] "to look at a way in which he could keep his government computers."

21. (U//FOUO) The C/DCI Administration's MFR indicated that on December 6, 1996, he spoke with [the then] Chief of the Administrative Law Division ⁴ (C/ALD) in OGC, to ask if Deutch could retain his Agency-issued, unclassified computer after leaving CIA. C/ALD reportedly said that he had concerns with government-owned property that was to be utilized for personal use. He advised that he would discuss the matter with the Principal Deputy General Counsel (PDGC).

⁴ (U//FOUO) This division has since been renamed the Administrative Law and Ethics Division.

22. (U//FOUO) On December 9, 1996, C/DCI Administration asked ISMS personnel to identify a system configuration which was identical to Deutch's. [He] hoped that Deutch would purchase a computer instead of retaining a government-owned computer.

23. (U//FOUO) According to a December 19, 1996 MFR signed by C/ALD and the PDGC, [C/ALD] discussed with [her] the request to loan computers to Deutch. ⁵ [She] mentioned the request to General Counsel Michael O'Neil, and stated:

The only legal way to loan the computers to the DCI would be if a contract was signed setting forth that John Deutch was a consultant to the CIA, and that the computers were being loaned to Mr. Deutch to be used solely for U.S. Government business.

⁵ (U//FOUO) According to his July 14, 1998 OIG interview, C/ALD prepared the MFR and it was co-signed by the PDGC and [him]. [He] stated that he took the only copy of it, sealed it in an envelope, and retained it. He sensed that it was likely there would eventually be an Inspector General investigation of the computer loan. [He] stated that this was the only time in his career that he has resorted to preparing such an MFR. He stated that he did not tell O'Neil about the MFR nor provide a copy to O'Neil since he judged that to be "unwise." He did not provide a copy of it to the OGC Registry. He said that he has kept it in his "hold box" since he wrote it.

24. (U//FOUO) Despite her reservations, the PDGC was told by O'Neil to work with C/DCI Administration to formulate a contract for Deutch to be an unpaid consultant. The contract would authorize the provision of a laptop computer for three months and a desktop computer for up to a year.

25. (U//FOUO) According to the MFR:

On or about 11 December, [the PDGC] was informed by [C/DCI Administration] that the DO wanted the computers loaned to him because they had the DO's personal financial data on them and he wanted access to that data. [C/DCI Administration] learned this information in conversation with the DCI. [The PDGC] informed [C/ALD] of this development, and they both agreed that it was improper to loan the computers to the DCI if the true purpose of the loan was to allow the DCI to have continued access to his personal information. [The PDGC] and [C/ALD] also expressed concern that the computers should not have been used by the DCI to store personal financial records since this would constitute improper use of a government computer. [C/ALD] held further conversations with [C/DCI Administration] at which time [C/ALD] suggested that the DCI's personal financial data be transferred to the DCI's personal computer rather than loaning Agency computers to the DCI. [C/DCI Administration] stated that this proposal would not work because the DCI did not own any personal computers. It was then suggested that the DCI be encouraged to purchase a personal computer and that the DCI personal financial records be transferred to the computer.

26. (U//FOUO) On December 10, 1996, a no-fee contract was prepared between John Deutch, Independent Contractor, and the CIA. Deutch was to provide consulting services to the DCI and senior managers, was to retain an Agency-issued laptop computer for three months, and would retain an Agency-issued desktop computer for official use for one year.

27. (U//FOUO) C/DCI Administration's MFR notes that on December 13, 1996, he spoke with O'Neil on the telephone. O'Neil directed that the contract being prepared for Deutch be modified to authorize Deutch two computers for a period of one year. The contract was revised on December 13, 1996; the reference to the laptop was deleted but Deutch was to retain two Agency-issued desktop computers and two STU-III secure telephones for one year.

28. (U//FOUO) According to the C/DCI Administration's MFR, on December 12, 1996, [he] again met with Deutch to discuss matters relating to Deutch's departure. The computer issue was again discussed:

I mentioned again that I had "strong reservations" about Mr. Deutch maintaining the Government-owned computers and restated that we would be happy to assist moving Mr. Deutch to a personally-owned platform. Mr. Deutch slammed shut his pen drawer on his desk and said thanks for everything without addressing the issue.

29. (U//FOUO) According to the C/ALD and PDGC MFR, they met with O'Neil on December 13, 1996 to discuss the loan of the computers to Deutch. [They] expressed concern that the loan of the computers would be improper if Deutch intended to use the computers for personal purposes. O'Neil stated that he had discussed the matter with Deutch, and Deutch knew he could not use the computers for personal purposes. O'Neil also stated, according to the MFR, that Deutch had his own personal computers and that Deutch would transfer any personal data from the CIA computers to his own. O'Neil said that the contract, which only called for the loan of two computers, had to be re-drafted so that it would cover the loan of a third computer. O'Neil advised that Deutch would not agree to an arrangement in which he would simply use his own computers for official work in place of a loaned CIA computer.⁶

⁶ (U//FOUO) The OIG investigation has not located any contract that includes a third

computer.

30. (U//FOUO) The PDGC recalls standing in the receiving line at a farewell function for Deutch and being told by Deutch's wife, "I can't believe you expect us to go out and buy another computer."

31. (U//FOUO) The MFR indicates that [the two OGC attorneys] dropped their objections to the loan of the computers, based on assurances from O'Neil that Deutch understood the computers would only be used for official purposes, and he would transfer his personal financial data to his own computer.

32. (U//FOUO) The contract was signed on December 13, 1996 by O'Neil and Deutch. The effective date for the contract was December 16, 1996. The contract states that Deutch "shall retain, for Government use only, two (2) Agency-issued desktop computers and two (2) STU-III's for the period of one year." Instead, Deutch was issued three PCMCIA cards and two PCMCIA card readers and all government-owned computers were returned to the Agency. On June 23, 1997, he purchased the cards and readers from CIA for \$1,476.

WHAT INFORMATION WAS FOUND ON DEUTCH'S MAGNETIC MEDIA?

- **How was the classified material discovered?**

33. (U//FOUO) Each of the two, unclassified, Agency-owned computers that were to be loaned to Deutch under the provisions of the December 13, 1996 contract were already located at Deutch's Maryland and Belmont residences. To effect the loan of the computers, C/DCI Administration, after consulting with Deutch and his personal assistant, requested that an Infosec Officer perform an inventory of the two government-owned Macintosh computers and peripherals at the Deutch residences. In addition, the Infosec Officer was to do a review to ensure no classified material had been accidentally stored on these computers. While at the Deutch residences, a contract engineer was to document the software applications residing on the computers and, at Deutch's request, install several software applications. This software included FileMaker Pro (e.g., a database) that was to be used with a calendar function and Lotus Notes that would be used with an address book. Deutch has no recollection of authorizing an inventory or a personal visit to his residences and questions the appropriateness of such a visit.

34. (U//FOUO) On December 17, 1996, the contract network engineer and the Infosec Officer, escorted by a member of the DCI security protective staff, entered Deutch's Maryland residence to conduct the review of the unclassified Macintosh computer and its peripherals. The Infosec Officer reviewed selected data on the computer and two PCMCIA cards, labeled unclassified, located in each of two PCMCIA card drives. Two other PCMCIA cards, one labeled unclassified and the other not labeled, were located on Deutch's desk.

35. (U//FOUO) The Infosec Officer's initial review located six files containing what appeared to be sensitive or classified information. Although the Infosec Officer believed that numerous other classified or sensitive files were residing on the computer, he concluded the system was now classified and halted his review. The contract network engineer agreed the system should be considered classified based on the information residing on the computer.

36. (U//FOUO) In addition to these six files, the contract network engineer and the Infosec Officer noted applications that allowed the Macintosh computer external connectivity via a FAX modem. The computer also had accessed the Internet via [an ISP], a DoD unclassified e-mail system, and [Deutch's bank] via its proprietary dial-up software.

- **What steps were taken to gather the material?**

37. (U//FOUO) The Infosec Officer telephoned C/DCI Administration and informed him of the

discovery of classified material. Although normal information security practice would have been to immediately confiscate the classified material and equipment, C/DCI Administration advised the Infosec Officer to await further instruction. [He] proceeded to contact then-CIA Executive Director Nora Slatkin. She referred him to O'Neil for guidance. [He] stated that he consulted with O'Neil, who "requested that we print off copies of the documents for his review." [He] contacted the Infosec Officer and instructed him to copy the six classified/ sensitive files to a separate disk and return to Headquarters. The Infosec Officer copied five of the six files.⁷

⁷ (U//FOUO) The Infosec Officer did not copy the sixth document, a letter to DCI nominee Anthony Lake that contained Deutch's personal sentiments about senior Agency officials.

38. (U//FOUO) After returning to Headquarters, the contract network engineer recalled being contacted by O'Neil. O'Neil advised that he had spoken with Deutch, and Deutch could not understand how classified information came to be found on the computer's hard drive. O'Neil wanted to know if any extraordinary measures were used to retrieve the classified documents and was told the documents were simply opened using Microsoft Word. O'Neil asked the contract network engineer to wait while Deutch was again contacted.

39. (U//FOUO) Shortly thereafter, the contract engineer stated that Deutch telephoned him and said he could not understand how classified information could have been found on the computer's hard drive as he had stored such information on the PCMCIA cards. The contract engineer told Deutch that the classified information had been found on the PCMCIA cards. The contract engineer recalled suggesting that Deutch might want a new hard drive and replacement PCMCIA cards to store unclassified files that could be securely copied from Deutch's existing PCMCIA cards. According to the contract engineer, Deutch agreed but wanted to review the PCMCIA card files first because they contained personal information.

40. (U//FOUO) On December 23, 1996, Deutch provided the four PCMCIA cards from his Maryland residence to the DCI Security Staff. These four cards were delivered to O'Neil the same day.

41. (U//FOUO) On December 27, 1996, the contract network engineer advised C/DCI Administration that two PCMCIA cards previously used by Deutch had been located in an office at Headquarters. One of the cards had an unclassified sticker and was labeled as "Deutch's Personal Disk." The other did not have either a classification sticker or a label. The files on the card with the unclassified sticker had been erased; however, the contract network engineer was able to recover data by the use of a commercially available software utility. Although labeled "unclassified," the contract network engineer noted that the files contained words such as "Secret," "Top Secret Codeword," "CIA," and the name of an Office of Development and Engineering facility. This discovery caused C/DCI Administration, on the advice of [the] Associate Deputy Director for Administration (ADDA),⁸ to contact O'Neil for assistance in expeditiously retrieving Deutch's Macintosh computers from the Maryland and Belmont residences.

⁸ (U//FOUO) The former ADDA retired in October 1997.

42. (U//FOUO) On the evening of December 27, 1996, the contract network engineer visited Deutch's Maryland residence, removed Deutch's hard drive, and delivered it to C/DCI Administration. On December 30, 1996, DCI Security Staff delivered to C/DCI Administration the hard drive from Deutch's Belmont residence. Both hard drives were then delivered to O'Neil.

43. (U//FOUO) On January 6, 1997, OPS/SIB, upon the approval of Slatkin, initiated an internal investigation to determine the security implications of the mishandling of classified information by Deutch.

44. (U//FOUO) According to Slatkin, she, O'Neil, and Richard Calder, Deputy Director for Administration had several discussions about how to proceed with the investigation. She also discussed with Acting DCI Tenet the issue of how to proceed. As a result, a select group was created to address this matter. Its purpose was to (1) take custody of the magnetic media that had been used by Deutch, (2) review Deutch's unclassified magnetic media for classified data, (3) investigate whether and to what extent Deutch mishandled classified information, and (4) determine whether classified information on Deutch's computers that had Internet connectivity was compromised.

45. (U//FOUO) By January 13, 1997, all hardware and files that had been used by Deutch, except four PCMCIA cards retrieved from Deutch's Maryland residence on December 23, 1996, were in SIB's possession. On February 3, 1997, O'Neil released the four PCMCIA cards to Calder, who transferred them to the group on February 4, 1997. Then-Director of Personnel Security (D/OPS) headed the group. Calder was the senior focal point for the group. In addition, a technical exploitation team was formed to exploit the magnetic media.

• **What steps were taken to recover information residing on Deutch's magnetic media?**

46. (U//FOUO) Five government-issued Macintosh computer hard drives and eight PCMCIA cards, used by Deutch and designated for unclassified purposes, were examined by a technical exploitation team within the group. Because each of the computers had modems, the PCMCIA cards were considered equally vulnerable when inserted into the card readers attached to the computers. The group had concerns that the processing of classified information on Deutch's five computers that were designated for unclassified information were vulnerable to hostile exploitation because of the modems. The group sought to determine what data resided on the magnetic media and whether CIA information had been compromised.

47. (U//FOUO) The examination of Deutch's magnetic media was conducted during the period January 10 through March 11, 1997. The technical exploitation team consisted of a Senior Scientist and two Technical Staff Officers, whose regular employment responsibilities concerned [data recovery]. The Infosec Officer who participated in the December 17, 1996 security inspection at Deutch's Maryland residence also assisted in the exploitation effort.

48. (U//FOUO) This team performed the technical exploitation of Deutch's magnetic media, recovered full and partial documents containing classified information, and printed the material for subsequent review. Technical exploitation began with scanning for viruses and making an exact copy of each piece of media used by Deutch. Further exploitation was performed on the copies. The original hard drives and PCMCIA cards were secured in safes. The copies were restored, in a read-only mode, on computers used by the team. Commercially available utility software was used to locate, restore, and print recoverable text files that had been erased. In an attempt to be exhaustive, the Senior Scientist wrote a software program to organize text fragments that appeared to have been part of word processing documents.

49. (U//FOUO) To accommodate concerns for Deutch's privacy, D/OPS was selected to singularly review all recovered data. He reviewed in excess of 17,000 pages of recovered text to determine which documents should be retained for possible future use in matters relating to the unauthorized disclosure of classified information.

50. (U//FOUO) Three of the PCMCIA cards surrendered by Deutch subsequent to the security inspection of December 17, 1996, were found to have characteristics that affected exploitation efforts. Specifically, the card labeled "John Backup" could not be fully exploited as 67 percent of the data was unrecognizable due to "reading" errors. The card labeled "Deutch's Disk" was found to have 1,083 "items" that were erased. The last folder activity for this card occurred on "December 20, 1996 at 5:51 [p.m.]." The third card, labeled "Deutch's Backup Disk" and containing files observed during the security inspection, was found to have been reformatted.⁹ The card was last modified on "December

20,1996, [at] 5:19 p.m."

⁹ (U//FOUO) Formatting prepares magnetic media for the storing and retrieval of information. Reformatting erases the tables that keep track of file locations but not the data itself, which maybe recoverable.

51. (U//FOUO) Subsequent investigation by OIG revealed that Deutch had paged the contract network engineer at 1000 hours on Saturday, December 21, 1996. In an e-mail to C/DCI Administration the following day, the contract network engineer wrote:

... he [Deutch] was experiencing a problem deleting files from one or (sic) his 170MB PCMCIA disks. As near as I [Contractor] can tell the disk has become corrupted and while it appears to allow him [Deutch] to copy files it did not allow him to delete them. We tried several techniques to get around the problem but none were successful. He [Deutch] indicated that he [Deutch] would continue to copy files and not worry about deleting any additional files. He [Deutch] asked what we were going to do with the disks he returned and I told him that we would in all probability degauss them and then physically destroy them

52. (U//FOUO) The exploitation efforts resulted in eight pieces of magnetic media yielding classified information. Of the eight pieces, four computers and three PCMCIA cards had prominent markings indicating that the equipment was for unclassified use.¹⁰ Forty-two complete documents [were classified up to Top Secret and a non-CIA controlled compartmented program] and 32 text or document fragments classified up to [TopSecret and a non-CIA controlled compartmented program] were recovered. Fourteen of the recovered classified documents contained actual printed classification markings (i.e., "SECRET," "Top Secret/ [a non-CIA controlled compartmented program]") as part of the document. These documents were located on hard drives and/or PCMCIA cards linked to Deutch's residences, 7th floor CIA office, and laptop.

¹⁰ (U//FOUO) OIG was unable to determine how the Belmont computer was marked because the chassis was disposed of prior to the OIG investigation.

53. (U//FOUO) Indications of Internet, [an ISP],¹¹ an unclassified Pentagon computer e-mail,¹² and online banking usage were found on several of the storage devices. A virus was found to have corrupted a file on the computer formerly located in Deutch's 7th floor CIA office. This computer was labeled "DCI's Internet Station Unclassified," but yielded classified information during the exploitation effort.

¹¹ (U//FOUO) In response to an authorization for disclosure signed by Deutch, [the ISP] provided business records to OIG. These records reflect that Deutch, using the screen name [that was a variation of his name,] maintained an account with [the ISP] since January 1, 1995.

¹² (U//FOUO) The Department of Defense recovered and produced in excess of 80 unclassified electronic message exchanges involving Deutch from May 1995 through January 1996. These messages reflect Deutch's electronic mail address as (variations of his name).

54. (U//FOUO) Recovered computer-generated activity logs reflect, in certain instances, classified documents were created by "John Deutch" during the period of June 1, 1995 and November 14, 1996. Many of the same documents, in varying degrees of completion, were found on different pieces of magnetic media. Additionally, the team recovered journals (26 volumes) of daily activities maintained by Deutch while he served at the DoD and CIA.

55. (U//FOUO) The following text box provides a summary of Deutch's magnetic media that resulted in the recovery of classified information.

UNCLASSIFIED//FOUO

MEDIA/LOCATION	MARKINGS	CONNECTED TO	INFORMATION RECOVERED
Quantum ProDrive Hard Drive/Deutch's Maryland Residence	"Unclassified" on Macintosh Power PC	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Six complete classified documents and text fragments including TS/Codeword. Internet, [ISP], [Deutch's bank], and DoD electronic mail usage. Indicators of visits to high risk Internet sites
Microtech PCMCIA Card/Deutch's Maryland Residence	"Deutch's Disk," "Unclassified," GS001414	PCMCIA Card Reader Networked to U.S. Robotics Fax Modem	Three complete classified documents and text fragments including TS/Codeword. [Bank] online usage. Card apparently reformatted on 12/20/96 at 5:51 p.m.
Microtech PCMCIA Card/Deutch's Maryland Residence	"Deutch's Backup Disk," "Unclassified," GS001490	PCMCIA Card Reader Networked to U.S. Robotics Fax Modem	31 complete classified documents and text fragments, five observed during security inspection. [Bank] Online Usage. Card apparently reformatted on 12/20/96 at 5:19 p.m.
Quantum ProDrive Hard Drive/Deutch's Belmont Residence	"JMD" on Drive Shell	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Six complete classified documents and text fragments including TS/Codeword. Internet usage. Indicators of visits to high risk Internet sites
Macintosh Power PC with Hard Drive/Deutch's 7th Floor Office, Original Headquarters Building	"Unclassified," "Property of O-DCL," "DCI's Internet Station Unclassified"	U.S. Robotics Fax Modem Two PCMCIA Card Readers	One complete classified document and text fragments including TS/Codeword. Word macro concept virus. Internet, DoD electronic mail usage.
Macintosh Power PC with Hard Drive/Deutch's OFOB Office	"Unclassified," "Property of DCI..."	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Text fragments including TS/Codeword. DoD electronic mail usage.
Macintosh Powerbook Laptop	"Dr. Deutch Primary," "Unclassified," "Property of DCI..."	Global Village Internal Modem	Two complete classified documents and text fragments including TS/Codeword.
Microtech PCMCIA Card/ISMS Office	"Deutch's Personal Disk," "Unclassified,"	N/A	Text fragments including TS/Codeword.

• What are some examples of the classified material that was found?

56. (U//FOUO) An October 7, 1996 memorandum from Deutch to the President and the Vice President, found on the hard drive of the Maryland residence computer, [contained information at the Top Secret/Codeword level]. The last paragraph of the memorandum notes [that the information is most sensitive and must not be compromised]:

Accordingly, with (National Security Advisor) Tony's [Lake] advice, I have restricted distribution of this information to Chris [Secretary of State Warren Christopher], Bill [Secretary of Defense William Perry], Tony [Lake], Sandy [Deputy National Security Advisor Sandy Berger], Leon Fuerth [the VP's National Security Advisor], and Louie Freeh with whom I remain in close touch.

57. (U//FOUO) [The] former Chief of Staff to the DCI and Slatkin both identified the memorandum as one Deutch composed on the computer at his Maryland residence in their presence on October 5, 1996.

58. (U//FOUO) In a memorandum to the President that was found on a PCMCIA card from the

Maryland residence, Deutch described an official trip. [The memorandum discussed information classified at the Top Secret level.]

59. (U//FOUO) In a memorandum to the President, which was found on a PCMCIA card from the Maryland residence, concerning a trip Deutch [discusses information classified at the Top Secret/Codeword level].

60. (U//FOUO) Deutch's memorandum to the President found on a PCMCIA card from the Maryland residence also [discusses a non-CIA controlled compartmented program].

61. (U//FOUO) An undated memorandum from Deutch to the President that was found on a PCMCIA card from the Maryland residence discusses a trip. [The memorandum discusses information classified at the Secret level.]

62. (U//FOUO) Another Deutch memorandum to the President that was found on a PCMCIA card from the Maryland residence [discusses information classified at the Secret/Codeword level].

63. (U//FOUO) In a memorandum to the President that was found on a PCMCIA card from the Maryland residence, Deutch [discusses information classified at the Top Secret/Codeword level].

64. (U//FOUO) [In] a memorandum with no addressee or originator listed, noted as revised on May 9, 1996 that was found on a PCMCIA card from the Maryland residence, [Deutch discusses information at the Secret level].

65. (U//FOUO) A document with no heading or date concerning a Deutch trip was found on the hard drive of Deutch's laptop computer which was marked for unclassified use, describes [information classified at the Secret/Codeword level].

66. (U//FOUO) A document without headings or dates, which was found on the hard drive of the unclassified computer in Deutch's 7th floor office, [discusses information classified at the Secret/Codeword level].

67. (U//FOUO) Deutch's journal, which was found on a PCMCIA card from the Maryland residence, also covered this topic but in more detail.

68. (U//FOUO) A spread sheet document [contains] financial [data] from fiscal year 1995 (FY95) through FY01 [which is classified at the Secret/compartmented program level. It was found on a PCMCIA card from the Maryland residence.

WHAT VULNERABILITIES MAY HAVE ALLOWED THE HOSTILE EXPLOITATION OF DEUTCH'S UNPROTECTED COMPUTER MEDIA?

69. (U//FOUO) The June 1994 *User's Guide for PC Security*, prepared by CIA's Infosec Officer Services Division, defines unclassified media as media that has never contained classified data. To maintain this status, all media and supplies related to an unclassified computer must be maintained separately from classified computer hardware, media, and supplies. Classified media is defined as media that contains or has contained classified data. It must be appropriately safeguarded from unauthorized physical (i.e., actually handling the computer) and electronic access (i.e., electronic insertion of exploitation software) that would facilitate exploitation. Computer media must be treated according to the highest classification of data ever contained on the media.

70. (U//FOUO) The *Guide* addresses vulnerabilities relating to computers. Word processors, other software applications, and underlying operating systems create temporary files on internal and external hard drives or their equivalents (i.e., PCMCIA cards). These temporary files are

automatically created to gain additional memory for an application. When no longer needed for memory purposes, the location of the files and the data saved on the media is no longer tracked by the computer. However, the data continues to exist and is available for future recovery or unwitting transfer to other media.

71. (U//FOUO) Additionally, data contained in documents or files that are deleted by the user in a standard fashion continue to reside on magnetic media until appropriately overwritten. These deleted files and documents can be recovered with commercially available software utilities. Furthermore, computers reuse memory buffers, disk cache, and other memory and media locations (i.e., slack and free space) on storage devices without clearing all previously stored information. This results in residual data being saved in storage space allocated to new documents and files. Although this data cannot be viewed with standard software applications, it remains in memory and can be recovered.

72. (U//FOUO) As a result of these vulnerabilities, security guidelines mandate procedures to prevent unauthorized physical and electronic access to classified information. An elementary practice is to separately process classified and unclassified information. Hard drives, floppy disks, or their equivalents used in the processing of classified information must be secured in approved safes and areas approved for secure storage when not in use. Individuals having access to media that has processed classified information must possess the appropriate security clearance. Computers that process classified information and are connected to a dial-up telephone line must be protected with a cryptographic device (e.g., STU-III) approved by NSA.

- **What was the electronic vulnerability of Deutch's magnetic media?**

73. (U//FOUO) Deutch used five government-owned Macintosh computers, configured for unclassified purposes, to process classified information. At least four of these computers were connected to modems that were lacking cryptographic devices and linked to the Internet, [an ISP], a DoD electronic mail server, and/or [bank] computers. As a result, classified information residing on Deutch's computers was vulnerable to possible electronic access and exploitation.

74. (U//FOUO) Deutch did receive e-mail on unclassified computers. One such message from France, dated July 11, 1995, was apparently from a former academic colleague who claimed to be a Russian.

75. (U//FOUO) Deutch's online identities used during his tenure as DO may have increased the risk of electronic attack. As a private subscriber [to an ISP], Deutch used a variant of his name for online identification purposes. He was also listed by true name in [the ISP's] publicly available online membership directory. This directory reflected Deutch as a user of Macintosh computers, a scientist, and as living in Bethesda, Maryland. Similarly, Deutch's online identity associated with CIA was:

johnd@odci[Office of DCI].gov[Government]

and with DoD, as:

deutch.johnd@odsdpo[Office of Deputy Secretary of DefensePostOffice].secdef[Secretary of Defense].osd.mil[Military].

After his confirmation as DCI, Deutch's DoD user identity was unobtainable from their global address database.

76. (U//FOUO) The technical exploitation team determined that high risk Internet sites had placed "cookies" ¹⁵ on the hard drives of the computers from Deutch's residences. According to DDA Calder, SIB's investigation demonstrated that the high risk material was accessed when Deutch was not present. These web sites were considered "risky" because of additional security concerns related

to possible technical penetration.

¹⁵ (U) A "cookie" is a method by which commercial web sites develop a profile of potential consumers by inserting data on the user's hard drive.

• **What was the physical vulnerability of Deutch's magnetic media?**

77. (U//FOUO) Deutch's government-issued computer at his primary residence in Maryland contained an internal hard drive and was lacking password protection. The drive was not configured for removal and secure storage when unattended even though classified information resided on the drive. Additionally, at the time of the December 17, 1996 security inspection, three of the four unsecured PCMCIA cards yielded classified information: two in PCMCIA readers and one on the desk in Deutch's study. An empty safe was also found with its drawer open.

78. (U//FOUO) Unlike his predecessors, Deutch declined a 24-hour security presence in his residence, citing concerns for personal privacy. Past practice for security staff, if present in a DCI's residence, was to assume responsibility for securing classified information and magnetic media. To compensate for the lack of an in-house presence, CIA security personnel and local police drove by Deutch's residence on a periodic basis. The two security chiefs responsible for Deutch's protective detail stated that Deutch was responsible for securing classified information in his residence. Deutch said that he thought his residence was secure. In hindsight, he said that belief was not well founded. He said he relied, perhaps excessively, on the CIA staff and security officials to help him avoid mistakes that could result in the unauthorized disclosure of classified information.

79. (U//FOUO) On May 16, 1995, Deutch approved the installation of a residential alarm system to include an alarm on the study closet. A one-drawer safe was placed in the alarmed closet. These upgrades were completed by early June 1995.

80. (U//FOUO) According to the first Security Chief assigned to Deutch, the alarm deactivation [was provided] code to a resident alien who performed domestic work at the Maryland residence. The alien [was permitted] independent access to the residence while the Deutch's were away. CIA security database records do not reflect any security clearances being issued to the alien. The resident alien obtained U.S. citizenship during 1998.

COULD IT BE DETERMINED IF CLASSIFIED INFORMATION ON DEUTCH'S UNCLASSIFIED COMPUTER WAS COMPROMISED?

81. (U//FOUO) According to the Senior Scientist who led the technical exploitation team, there was "no clear evidence" that a compromise had occurred to information residing on storage devices used by Deutch. In a February 14, 1997 MFR, the Senior Scientist concluded:

A complete, definitive analysis, should one be warranted, would likely take many months or longer and still not surface evidence of a data compromise.

82. (U//FOUO) On May 2, 1997, the Chief, SIB wrote in a memorandum to the Director of OPS:

In consultation with technical experts, OPS investigators determined the likelihood of compromise was actually greater via a hostile entry operation into one of Mr. Deutch's two homes (Bethesda, Maryland and Boston, Massachusetts) to "image" the contents of the affected hard drives Due to the paucity of physical security, it is stipulated that such an entry operation would not have posed a particularly difficult challenge had a sophisticated operation been launched by opposition forces The Agency computer experts advised that, given physical access to the computers, a complete "image" of the hard drives could be made in [a short amount of time].

WHAT KNOWLEDGE DID DEUTCH HAVE CONCERNING VULNERABILITIES ASSOCIATED WITH COMPUTERS?

• What is Deutch's recollection?

83. (U//FOUO) During an interview with OIG, Deutch advised that, to the best of his recollection, no CIA officials had discussed with him the proper or improper use of classified and unclassified computers. Around December 1997, approximately one year after he resigned as DCI, he first became aware that computers were vulnerable to electronic attack. Not until that time, Deutch commented, had he appreciated the security risks associated with the use of a modem or the Internet in facilitating an electronic attack.¹⁶

¹⁶ (U//FOUO) After reading the draft ROI, Deutch's refreshed recollection is that it was in December 1996, not December 1997, that he first became aware that his computer priorities resulted in vulnerability to electronic attack.

84. (U//FOUO) Although stating that he had not received any CIA security briefings relating to the processing of information on computers, Deutch acknowledged that classified information must be properly secured when unattended. Specifically, he stated, "I am completely conscious of the need to protect classified information."

85. (U//FOUO), In response to being advised that classified information had been recovered from government computers configured for his unclassified work, Deutch stated that he "fell into the habit of using the [CIA] unclassified system [computers] in an inappropriate fashion." He specifically indicated his regret for improperly processing classified information on the government-issued Macintosh computers that were connected to modems. Deutch acknowledged that he used these government-issued computers to access [the ISP], [his bank], the Internet, and a DoD electronic mail server.

86. (U//FOUO) Deutch indicated he had become accustomed to exclusively using an unclassified Macintosh computer while serving at DoD. He acknowledged that prior to becoming DCI, he was aware of the security principle requiring the physical separation of classified and unclassified computers and their respective information. However, he said he believed that when a file or document was deleted (i.e., dragged to the desktop trash folder), the information no longer resided on the magnetic media nor was it recoverable. Deutch maintained that it was his usual practice to create a document on his desktop computers, copy the document to an external storage device (e.g., floppy disk), and drag the initial document to the trash folder.

87. (U//FOUO) During his tenure as DCI, Deutch said that he intentionally created the most sensitive of documents on computers configured for unclassified use. Deutch stated that if these documents were created on the classified CIA computer network, CIA officials might access the system at night and inappropriately review the information. Deutch said that he had not spent a significant amount of time thinking about computer security issues.

88. (U//FOUO) Deutch advised that other individuals had used the government computer located in the study of his Maryland residence. Deutch's wife used this computer to prepare reports relating to official travel with her husband. Additionally, [another family member] used this computer to access [a university] library. Regarding the resident alien employed at the Maryland residence, Deutch indicated that, to his knowledge, this individual never went into the study. He further believed that the resident alien normally worked while Mrs. Deutch was in the residence.

• What did Deutch learn at [an] operational briefing?

89. (U//FOUO) On August 1, 1995, Deutch and several senior CIA officials receive[d] various

operational briefings.

90. (U//FOUO) [During these briefings] Deutch was specifically told that data residing on a [commercial ISP network was vulnerable to a computer attack.]

91. (U//FOUO) Deutch did not have a specific recollection relating to the August 1, 1995 briefing. He could not recall making specific comments to briefers concerning his use of [his ISP] and the need to switch to another ISP.

- **What was Deutch's Congressional testimony?**

92. (U//FOUO) On February 22, 1996, DCI Deutch testified before the Senate Select Committee on Intelligence on the subject of worldwide security threats to the United States during the post-Cold War era. During his appearance, Deutch stated:

Mr. Chairman, I conclude with the growing challenge of the security of our information systems. There are new threats that come from changing technologies. One that is of particular concern to me is the growing ease of penetration of our interlocked computer and telecommunications systems, and the intelligence community must be in the future alert to these needs-- alert to these threats.

93. (U//FOUO) On June 25, 1996, DCI Deutch testified in front of the Permanent Investigations Subcommittee of the Senate Governmental Affairs Committee. The Committee was investigating the vulnerability of government information systems to computer attacks. Deutch's testimony focused on information warfare, which he defined as unauthorized foreign penetrations and/or manipulation of telecommunications and computer network systems.

94. (U//FOUO) In his prepared statement submitted to the Committee, Deutch indicated:

like many others in this room, [I] am concerned that this connectivity and dependency [on information systems] make us vulnerable to a variety of information warfare attacks These information attacks, in whatever form, could ... seriously jeopardize our national or economic security I believe steps need to be taken to address information system vulnerabilities and efforts to exploit them. We must think carefully about the kinds of attackers that might use information warfare techniques, their targets, objectives, and methods Hacker tools are readily available on the Internet, and hackers themselves are a source of expertise for any nation or foreign terrorist organization that is interested in developing an information warfare capability We have evidence that a number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks.

- **What are the personal recollections of DO staff members?**

95. (U//FOUO) Deutch's [Executive] Assistant served in that position from February 1995 through July 1996 at DoD and CIA. [He] considered Deutch to be an "expert" computer user. [The Executive Assistant] was responsible for coordinating the preparation of computers for Deutch's use upon his confirmation as DCI. During the transition, [the Executive Assistant] informed Deutch that the processing of classified and unclassified information required the use of separate computers to prevent the improper transfer of data. [The Executive Assistant] stated that the computer support staff at CIA went to great lengths to appropriately label Deutch's computers as either classified or unclassified in order to prevent improper use.

96. (U//FOUO) [The Executive Assistant] advised that he never informed Deutch that it was permissible to process classified information on a computer configured for unclassified use. [The Executive Assistant] stated that he was not aware that Deutch processed classified information on

computers configured for unclassified use. When advised that classified material had been recovered from multiple computers used by Deutch that had been configured for unclassified purposes, [the Executive Assistant] responded that he was at a loss to explain why this had occurred.

97. (U//FOUO) [The Executive Assistant] remembered the August 1, 1995 briefing. [The Executive Assistant] said that Deutch was very concerned about information warfare and, specifically, computer systems being attacked. [The Executive Assistant] recalled that during his CIA tenure, Deutch and he became aware of efforts by [others] to attack computer systems.

98. (U//FOUO) The computer specialist who provided regular information support to Deutch while he served at DoD, was hired at Deutch's request in June 1995 to provide computer support to the DCI Area. After arriving at CIA, the computer specialist provided direct computer support to Deutch about once per week. At times, Deutch, himself, would directly contact the computer specialist for assistance.

99. (U//FOUO) The computer specialist described Deutch as a "fairly advanced" computer user who sought and used software that was considered to be above average in complexity. Deutch was further described as having "more than a passing interest in technology" and asking complex computer-related questions. The computer specialist found that Deutch "kept you on your toes" with questions that required research [for] the answers. Deutch was also described as having a heightened interest in the subject of encryption for computers. The computer specialist recalled that all computer equipment issued to Deutch was appropriately labeled for classified or unclassified work.

100. (U//FOUO) The computer specialist remembered a conversation with Deutch on the subject of computer operating systems creating temporary documents and files. This conversation occurred while the computer specialist restored information on Deutch's computer after it had failed (i.e., crashed). Deutch watched as documents were recovered and asked how the data could be restored. Deutch was also curious about the utility software that was used to recover the documents. The computer specialist explained to Deutch that data was regularly stored in temporary files and could be recovered. Deutch appeared to be "impressed" with the recovery process.

101. (U//FOUO) During another discussion, the computer specialist recalled telling Deutch that classified information could not be moved to or processed on an unclassified computer for security reasons.

102. (U//FOUO) The computer specialist considered Deutch to be a knowledgeable Internet user who had initially utilized this medium while a member of the scientific community at the Massachusetts Institute of Technology. During September 1996 and while Deutch was still serving as DCI, the unclassified CIA Internet web page was altered by a group of Swedish hackers. During discussions with the computer specialist concerning this incident, Deutch acknowledged that the Internet afforded the opportunity for the compromise of information.

103. (U//FOUO) C/ ISMS, who supervised computer support provided to Deutch from the time of his arrival at CIA through October 1996, considered Deutch to be a computer "super user." Deutch only sought assistance when computer equipment was in need of repair or he desired additional software. The computer support supervisor stated that all unclassified computers and PCMCIA cards that were provided for Deutch's use had green labels indicating they were for unclassified purposes.

104. (U//FOUO) The LAN technician, who initially configured Deutch's computers at CIA, stated that he labeled all equipment to reflect whether it was designated for classified or unclassified purposes. The technician's stated purpose was to make it clear to Deutch what information could be processed on a particular computer given the requirement that Deutch have access to both classified and unclassified computers.

HAD DEUTCH PREVIOUSLY BEEN FOUND TO HAVE MISHANDLED CLASSIFIED INFORMATION?

105. (U//FOUO) Beginning in 1977, when he was the Director of Energy Research at the Department of Energy (DoE), Deutch had a series of positions with U.S. Government agencies that required proper handling and safeguarding of classified information to include sensitive compartmented information and DoE restricted data.

106. (U//FOUO) From 1982 to 1988, Deutch was a paid consultant to the CIA's National Intelligence Council. In 1984, he was also under contract to the CIA's Directorate of Intelligence, Office of Scientific Weapons and Research, serving as a member of the DCI's Nuclear Intelligence Panel.

107. (U//FOUO) [CIA records reflect Deutch had problems before becoming Director with regard to the handling of classified information. Other specific information on security processing and practices has been deleted due to its level of classification.] Deutch served as DoD's Undersecretary for Acquisitions and Technology and Deputy Secretary of Defense prior to his appointment as DCI.

108. (U//FOUO) On November 21, 1995, DCI Deutch signed a CIA classified information non-disclosure agreement concerning a sensitive operation. Several provisions pertain to the proper handling of classified information and appear to be relevant to Deutch's practices:

I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information,

I have been advised that ... negligent handling of classified information by me could cause damage or irreparable injury to the United States

I have been advised that any breach of this agreement may result in the termination of any security clearances I hold; removal from any position or special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances

I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access ... upon the conclusion of my employment

I have read this Agreement carefully and my questions, if any, have been answered.

OIG also obtained similar, non-disclosure agreements signed by Deutch during his employment at DoD.

WHAT LAWS, REGULATIONS, AGREEMENTS, AND POLICIES HAVE POTENTIAL APPLICATION?

109. (U) Title 18 United States Code (U.S.C.) § 793, "Gathering, transmitting or losing defense information" specifies in paragraph (f):

Whoever, being entrusted with or having lawful possession or control of any document, writing,... or information, relating to national defense ... through gross negligence permits the same to be removed from its proper place of custody ... shall be fined under this title or imprisoned not more than ten years, or both.

110. (U) Title 18 U.S.C. § 798, "Disclosure of classified information" specifies in part:

Whoever, knowingly and willfully ... uses in any manner prejudicial to the safety or interest of the United States ... any classified information ... obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes ... shall be fined under this title or imprisoned not more than ten years, or both.

111. (U) Title 18 U.S.C. § 1924, "Unauthorized removal and retention of classified documents or material" specifies:

Whoever, being an officer, employee, contractor or consultant of the United States, and, by virtue of his office, employment, position or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined not more than \$1,000, or imprisoned for not more than one year, or both.

112. (U) The National Security Act of 1947, CIA Act of 1949, and Executive Order (E.O.) 12333 establish the legal duty and responsibility of the DCI, as head of the United States intelligence community and primary advisor to the President and the National Security Council on national foreign intelligence, to protect intelligence sources and methods from unauthorized disclosure.

113. (U) Director of Central Intelligence Directive (DCID) 1/16, effective July 19, 1988, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," reiterates the statutory authority and responsibilities assigned to the DCI for the protection of intelligence sources and methods in Section 102 of the National Security Act of 1947, E.O.s 12333 and 12356, and National Security Decision Directive 145 and cites these authorities as the basis for the security of classified intelligence, communicated or stored in automated information systems and networks.

114. (U) DCID 1/21, effective July 29, 1994, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)" specifies in paragraph 2:

All [Sensitive Compartmented Information] must be stored within accredited SCIFs. Accreditation is the formal affirmation that the proposed facility meets physical security standards imposed by the DCI in the physical security standards manual that supplements this directive.

115. (U//FOUO) Headquarters Regulation (HR) 10-23, Storage of Classified Information or Materials. Section C (1) specifies:

Individual employees are responsible for securing classified information or material in their possession in designated equipment and areas when not being maintained under immediate personal control in approved work areas.

116. (U//FOUO) HR 10-24, "Accountability and Handling of Collateral Classified Material," prescribes the policies, procedures, and responsibilities associated with the accountability and handling of collateral classified material. The section concerning individual employee responsibilities states:

Agency personnel are responsible for ensuring that all classified material is handled in a secure manner and that unauthorized persons are not afforded access to such material.

117. (U//FOUO) HR 10-25, "Accountability and Handling of Classified Material Requiring Special Control," sets forth policy, responsibilities, and procedures that govern the transmission, control, and

storage of Restricted Data, treaty organization information, cryptographic materials, and Sensitive Compartmented Information. The section states:

Individuals authorized access to special control materials are responsible for observing the security requirements that govern the transmission, control, and storage of said materials. Further, they are responsible for ensuring that only persons having appropriate clearances or access approvals are permitted access to such materials or to the equipment and facilities in which they are stored.

HOW WAS A SIMILAR CASE HANDLED?

118. (U//FOUO) In November 1996, a senior CIA official was determined to have routinely authored CIA unique, classified documents on his personal home computer and CIA-issued laptop computer configured for unclassified use. Some of the documents were at the Secret and Top Secret/Codeword level. In addition, the senior Agency official had used both computers to visit Internet sites. In addition, the senior official's family members had access to both computers. However, there was no way to determine if the computer hard drives had been compromised.

119. (U//FOUO) On December 12, 1996, [the] OPS Legal Advisor, referred a crimes report to the Associate General Counsel (AGC) in the CIA Office of General Counsel. On December 13, 1996, the AGC forwarded to DoJ a crimes report on this incident. In June 1997, a Personnel Evaluation Board (PEB) decided to downgrade the official from an SIS-06 to SIS-05, issue a two-year letter of reprimand including caveats against monetary and non-monetary awards and promotions, and suspend the official for 30 workdays without pay. In addition, the PEB directed the Office of Congressional Affairs to brief the appropriate Congressional intelligence committees about this senior official's breach of security. On September 11, 1997, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence were briefed on this incident by Executive Director David Carey.

WHAT ACTIONS DID SENIOR AGENCY OFFICIALS TAKE IN HANDLING THE DEUTCH CASE?

- **What actions were taken by senior Agency officials after learning of this matter?**

120. (U//FOUO) After learning from O'Neil on December 17, 1996 that classified information had been discovered at Deutch's Maryland residence, Slatkin brought the issue to the attention of Acting DCI George Tenet within one day. She asserted there were multiple discussions with Tenet over time and "everything" had his concurrence. Slatkin explained that the issue was too sensitive for her and Tenet had the responsibility for making the decisions relating to the Deutch incident. Slatkin stated she was also concerned that others may have perceived that she and O'Neil, due to their close association with Deutch, should recuse themselves from the matter. Slatkin said that Tenet gave her the responsibility for coordinating this matter. She relied on O'Neil for legal advice and Calder for a technical review.

121. (U//FOUO) Calder recalled one or possibly two "late night discussions" with Tenet concerning the Deutch incident. One meeting was to provide Tenet "the lay of the land." At the second meeting, Tenet gave instructions for the investigation to proceed unimpeded.

122. (U//FOUO) Tenet stated he first learned of the discovery of classified information on the Maryland computer in December 1996 or January 1997 from either the Chief, DCI Security Staff or from the C/DCI Administration. Tenet recalled that Slatkin and O'Neil got involved in deciding how to handle the issue. Tenet did not hear about any disagreements concerning the handling of this matter and believed that Slatkin and O'Neil did not want to place Tenet in the position of adjudicating a matter involving Deutch.

123. (U//FOUO) O'Neil stated that he is uncertain how he first learned of the discovery of classified information on Deutch's Maryland computer. However, according to C/DCI Administration, a meeting was held on the afternoon of December 17, 1996 with O'Neil. At that meeting, O'Neil stated Deutch was concerned about retaining his personal information before returning the four PCMCIA cards to CIA. C/DCI Administration offered a solution by offering to provide Deutch with replacement PCMCIA cards on which Deutch could transfer his personal information. O'Neil passed this suggestion to Deutch, and Deutch agreed. Afterward, the contract network engineer also talked to Deutch about copying his personal information to the new PCMCIA cards. The contract network engineer recalled Deutch wanting to review the files on the original PCMCIA cards because they contained personal information. ¹⁷

¹⁷ (U//FOUO) in his interview with OIG, Deutch confirmed he reviewed the original PCMCIA cards to delete personal information.

124. (U//FOUO) [The] PDGC learned of the matter on the day of its discovery. Between that date, December 17, 1996, and the date SIB began its investigation, the PDGC recalled there was an ongoing dialogue involving O'Neil, Slatkin, and Calder. The PDGC stated that O'Neil kept her abreast of developments.

125. (U//FOUO) The former ADDA believes that C/DCI Administration initially apprised her of the discovery on December 26, 1996. Her first concern related to properly securing the classified information at the Deutch residence, which the C/DCI Administration said he would handle. Several days later, [she] learned that the magnetic media at the Maryland residence had been secured, although not as expeditiously as she desired. [She] stated that the PCMCIA cards that had been in Deutch's possession were given to O'Neil.

126. (U//FOUO) The former ADDA stated that Calder, Slatkin, and O'Neil held a series of meetings to discuss how to handle the incident. She recalled other issues surfacing, such as the resident alien employed as a maid at the Deutch residence; Deutch's personal financial records being maintained on government-owned computers; "disks" Deutch carried in his shirt pocket; and other government-issued unclassified computers at Deutch's Belmont residence, the OEOP, and Headquarters that may contain classified information.

127. (U//FOUO) D/OPS was first briefed on the case by Calder, who became [his] senior focal point with the former ADDA serving as a back-up. D/OPS never discussed the case directly with either Slatkin or O'Neil. He remembered that the specific permission of Slatkin or O'Neil was needed to involve others in the case. According to D/OPS, the former ADDA believed that Slatkin and O'Neil had as their main concern the fear that sensitive and personal information contained in Deutch's journals would leak. Slatkin stated it was standard operating procedure, when dealing with sensitive investigations or operations, to review requests to involve additional individuals. She claimed it was common practice for her to review such requests with the DCI. She does not recall denying any request to involve others in this case.

128. (U//FOUO) According to C/SIB, D/OPS asked him to conduct a security investigation to determine: (1) if classified information found on Deutch's government-issued unclassified computer had been compromised, and (2) what conditions would allow a compromise to occur. C/SIB said he was to determine the "who, what, where, when, and why." C/SIB expected "noteworthy" information would be compared to the appropriate DCID security standards and adjudication would be based on SIB's findings. He recalled advising the D/OPS that classified information on unclassified media could involve a potential violation of federal law.

129. (U//FOUO) The OPS Legal Advisor wrote in a January 7, 1997 MFR that he attended a meeting the previous day with Calder, D/OPS, C/SIB, and an SIB investigator to discuss the discovery of the classified information on the computer at Deutch's Maryland residence. Among the issues discussed.

were:

Acknowledgment that because this case involves former DCI Deutch, whatever actions are taken by OPS and other parties will be scrutinized very closely. Therefore, it was stressed by everyone at the meeting that the security investigation of this case must follow the same pattern established in other cases where employees have placed classified information on a computer and possibly exposed that information to access by unauthorized individuals.

130. (U/ FOUO) Calder stated that the OPS Legal Advisor was strident in his concern that Deutch be treated the same as any other Agency employee and senior officials should scrupulously avoid showing special treatment to Deutch. Calder agreed that the investigation should resemble those conducted for similar violations by other Agency personnel. He stated he was concerned that he insulate the OPS/SIB personnel and the C/DCI Administration to ensure that they did not "get ground up."

131. (U/ FOUO) Calder stated that he initially assumed this matter would arise again in the future, possibly with a Congressional committee. Therefore, he insisted that the case be conducted in the same manner as for any CIA employee.

- **How were the Maryland PCMCIA cards handled?**

132. (U/ FOUO) SIB sought to obtain and secure all the government-issued computer equipment and magnetic media that had been provided to Deutch, such as the computers and peripherals that were at both Deutch residences. By early January 1997, all government-issued computer equipment and magnetic media used by Deutch had been turned over to SIB with the exception of the four PCMCIA cards that had been observed by the inspection team on December 17, 1996.

133. (U/ FOUO) O'Neil recalled that a DCI Security officer brought him the four PCMCIA cards from the Maryland residence. O'Neil stated he put the PCMCIA cards in his safe and never opened the envelope that contained them. He said he gave the PCMCIA cards to Calder without argument when asked.

134. (U/ FOUO) Calder recalled that O'Neil told him that Deutch wanted the PCMCIA cards destroyed. Calder advocated the position that the cards should not be tampered with and must be maintained in the event of a future leak investigation. According to Calder, O'Neil and Deutch came to realize the PCMCIA cards could not be summarily destroyed. Calder stated that he went to O'Neil on three or four occasions in an attempt to obtain the four PCMCIA cards, and it took two to three weeks to reach a satisfactory arrangement for O'Neil to surrender them.

135. (U/ FOUO) The PDGC also recalled, "We had to hammer O'Neil to give the [PCMCIA] cards to Security." The PDGC believes Slatkin, whose "loyalty to Deutch was incredible," and Deutch pressured O'Neil not to allow others to have access to the personal information on the cards. The PDGC stated that she, Calder, the OPS Legal Advisor, and C/ SIB "pushed the other way" and advocated that O'Neil turn the cards over to Security. C/SIB confirmed the difficulty obtaining the four PCMCIA cards in O'Neil's possession.

136. (U/ FOUO) The former ADDA recalled advising Slatkin that the investigation was dragging on, and that unidentified individuals believed that this was being done purposely in order to "cover up" the event. The former ADDA told Slatkin that O'Neil's withholding of the four cards supported the "cover up" perception.

137. (U/ FOUO) According to Slatkin, after the former ADDA told Slatkin about the problem with the four remaining disks, she requested a meeting with Tenet, O'Neil, and Calder. Tenet reportedly told O'Neil to surrender the PCMCIA cards to Calder. Calder stated that O'Neil claimed that, although

Calder had discussed his need for the cards, Calder had never specifically asked O'Neil to turn them over. C/ SIB states that Calder, in his presence, "specifically ask[ed]" O'Neil to release the PCMCIA cards. Slatkin said she would have reacted earlier if she had known of Calder's concern.

138. (U/ /FOUO) According to O'Neil, he, Tenet, Slatkin, and Calder had conversations over a period of several weeks on the exploitation of the PCMCIA cards and protecting Deutch's privacy. After Tenet decided on the process for handling the cards, they were delivered to Calder. O'Neil said he never refused to turn over the cards for exploitation.

139. (U/ /FOUO) O'Neil surrendered the four PCMCIA cards to Calder on February 3, 1997. Calder provided the cards to C/SIB on February 4, 1997.

- **What was the course of the Special Investigations Branch's investigation of Deutch?**

140. (U/ /FOUO) Calder stated that, in his view, Slatkin and O'Neil did not want Deutch's name "to be besmirched" and O'Neil assumed the role of an "interlocutor." He also said that Slatkin and O'Neil were particularly sensitive that a possible vendetta would be orchestrated by security personnel as a response to interference by O'Neil and Slatkin in a previous, unrelated, joint investigation involving the DoD.¹⁸ Calder characterized his encounters with Slatkin regarding the Deutch investigation as "always difficult discussions" and that it was continually necessary to "push forward" and achieve "a negotiated peace." Slatkin, however, stated that she had no involvement in the DoD-CIA investigation except to determine why the Acting Director and she had not been informed of the notification to DoD.

¹⁸ (U/ /FOUO) Based on a series of intelligence leaks in the *Washington Times*, CIA's Special Investigations Branch determined the leaks were related to the distribution of intelligence reports at the Pentagon. In a routine procedure, CIA sent a letter to DoD and the Defense Intelligence Agency (DIA) to coordinate an investigation. According to Calder, the DIA nominee for Director of that organization contacted Slatkin and demanded an explanation of the CIA's actions. Subsequently, O'Neil requested that DDA Calder rescind the CIA letter. Calder states that O'Neil commented the actions of CIA security officials appeared to be "vindictive and malicious."

141. (U/ /FOUO) The OPS Legal Advisor believes Slatkin "constrained the investigative apparatus." He cited, as an example, Slatkin advocating allowing Deutch to go into the files to determine if the information was personal or belonged to the CIA. The OPS Legal Advisor stated that the policy has always been that an individual who places personal information on a government computer loses the expectation of privacy and the material reverts to the control of the government authorities. The OPS Legal Advisor stated that Calder, D/OPS, and the former ADDA tried to keep the investigation on track. Slatkin denied interfering with the investigation. She stated that she did not make any unilateral decisions about the course of the investigation. All requests made by Deutch were relayed to O'Neil, Calder, and Tenet.

142. (U/ /FOUO) In the early stages of SIB's investigation, Calder recalled telling Tenet there was no indication of a compromise and the investigation was proceeding. Calder said that the investigators showed him some of the classified material. It included Top Secret/ [Codeword] information; collection methods and imagery; and possibly information identifying CIA operations officers.

143. (U/ /FOUO) Calder stated that after a complete package of Deutch's material was recovered from the magnetic media, the question arose as to the proper person to review the material. Because the material contained personal information, Calder recalled that Deutch wanted to review the material himself or have O'Neil do the review. Ultimately, Slatkin selected D/OPS for the task.

144. (U/ /FOUO) As part of the SIB investigation, C/SIB interviewed staff from DCI Security and the

DCI Information Services Management Staff; he also planned to interview [Deutch's Executive Assistant] and Deutch.¹⁹ On March 24, 1997, Calder informed C / SIB that C/SIB would not be the one to interview Deutch. (Calder later explained to OIG investigators that a concern existed to have somebody who was politically sensitive question Deutch, should such an interview prove necessary.) At Calder's request, SIB composed questions to ask Deutch and, on May 15, 1997, forwarded them to D/OPS for review. However, C/SIB also informed Calder that SIB would not continue their efforts because certain interviewees (i.e., Deutch) were not accessible to SIB. Calder agreed.

¹⁹ (U//FOUO) C/SIB noted that he did not review Deutch's official security file. OIG reviewed the file.

145. (U//FOUO) The OPS Legal Advisor stated that, normally, a case similar to Deutch's would not only be referred to SIB for investigation, but a contemporaneous damage assessment would also be conducted. If the subject was a former employee, typically the subject would be banned from holding a security clearance and future CIA employment.

146. (U//FOUO) After D/OPS reviewed the 17,000 pages of recovered documents, he prepared a report of his findings and attached a copy of C/SIB's separate, signed report. He recalled receiving a "panicky" call from the former ADDA relaying that Slatkin wanted the report immediately.

147. (U//FOUO) Calder was familiar with D/OPS's report and stated that it was the lone document that he retained following the conclusion of the investigation. He recalled sending the report to Slatkin and receiving it back with marginal comments, possibly asking if the PCMCIA cards had been destroyed. Slatkin recalled that the draft report was hand-carried to her by Calder. After she read the report, she made written editorial comments requesting clarification and returned the draft report to either Calder or D/OPS. She received the final report, reviewed it, and personally handed it to Tenet. Tenet does not remember ever seeing D/OPS's report, nor does he recall any of the details of the report. He said it is possible that someone told him about the report or showed it to him.

148. (U//FOUO) A signed copy of the D/OPS report dated July 8, 1997, was recovered from the DDA's Registry. It did not have any notes on the text or attached to the document. No copy was ever recovered from the DCI's Executive Registry, the Executive Director's Office, Calder's personal safe, or anywhere in OGC.

149. (U//FOUO) There was considerable discussion of what should be done with the magnetic media after its material was catalogued. O'Neil said that Tenet's decision was to retain permanently the PCMCIA cards and a copy of all the classified documents. Calder, however, said there was some disagreement among the parties and the ultimate decision was to destroy the material, including the magnetic media. At the end of the investigation, Calder remembered asking D/OPS what happened to the PCMCIA cards and being told the disks were about to be destroyed or had been destroyed. Nevertheless, Calder said he was not certain the cards were destroyed.

150. (U//FOUO) After D/OPS sent his report to Calder, the OPS Legal Advisor received an e-mail from the C/ALD stating that the PDGC had spoken to Calder about the SIB investigation of Deutch. Calder reportedly said Deutch would be given a code of conduct briefing in conjunction with Deutch's security briefing as a member of the Proliferation Commission.²⁰ On August 3, 1997, the OPS Legal Advisor sent the C/ALD an e-mail response expressing concern that no one at DoD or the White House had, so far, been notified about a possible compromise of information. He also raised the issue of Deutch retaining his security clearance. The OPS Legal Advisor wrote:

I remain unpersuaded, however, that the CIA has done everything it can in this case to protect CIA and DOD equities. The investigation has been one in name only I'm certainly not persuaded that giving this man a security clearance is in the best interest of the U.S. Government or the President I mean, geez, when was the last time a subject of an

investigation was not interviewed because he objected to talking to security officers and the EXDIR, a personal friend, used her position to short circuit an investigation? Let's be honest with each other, this so-called investigation has been handled in a manner that was more designed not to upset friendships than to protect the interests of the U.S.G.

²⁰ (U/ /FOUO) There is no record of Deutch receiving a code of conduct briefing. The Center for CIA Security provided an SCI briefing to the commission members on two occasions. Deutch was present for the second one-hour presentation on November 17, 1998.

151. (U/ /FOUO) C/SIB had also relayed his concerns about the possible exposure of DoD classified material of ongoing military operations. In his chronology, C/SIB wrote that on March 14, 1997, Calder decided appropriate senior level DoD officials should be briefed on a potential compromise. Calder planned to brief Slatkin of this decision. C/ SIB indicated he again reminded Calder of the need for DoD notification on March 24, 1997. The OIG investigation did not locate any information that such notification occurred until OIG notified DoD on June 17, 1998.

152. (U/ /FOUO) As of May 1998, when OIG began its investigation, there was no information in Deutch's official Agency security file concerning the SIB investigation or its findings nor was there any evidence of a security adjudication.

SHOULD A CRIMES REPORT INITIALLY HAVE BEEN FILED ON DEUTCH IN THIS CASE?

153. (U) Title 28 U.S.C. § 535, "Investigation of crimes involving Government officers and employees," requires that

any information, allegation or complaint received in a department or agency of the executive branch of the government relating to violations of Title 18 [U.S. Code] involving Government officers and employees shall be expeditiously reported to the Attorney General.

154. (U) Section 1.7(a) of E.O. 12333, United States Intelligence Activities, requires senior officials of the intelligence community to "report to the Attorney General possible violations of federal criminal laws by employees and [violations] of specified criminal laws by any other person " This responsibility is to be carried out "as provided in procedures agreed upon by the Attorney General and the head of the department or agency concerned...."

155. (U/ /FOUO) Pursuant to Part 1.7(a) of E.O. 12333, the DCI and the Attorney General agreed on crimes reporting procedures for CIA on March 2, 1982. These procedures, which are included as Annex D to HR 7-1, were in effect from that time until August 2, 1995, when they were superseded by new procedures.²¹ The new procedures are contained in a document, "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," signed by DCI Deutch.

²¹ (U/ /FOUO) Although HR 7-1 Annex D was superseded by the MOU on August 2, 1995, the current version of HR 7-1 Annex D is dated December 23, 1987 and does not reflect the changes caused by the subsequent MOU.

156. (U/ /FOUO) According to the Memorandum of Understanding (MOU),

[w]hen the General Counsel has received allegations, complaints, or information (hereinafter allegations) that an employee ²² of the Agency may have violated, may be violating, or may violate a federal criminal statute, that General Counsel should within a reasonable period of time determine whether there is a reasonable basis ²³ to believe that a federal crime has been, is

being, or will be committed and that it is a crime which, under this memorandum, must be reported.²⁴

²² (U//FOUO) According to paragraph II B. 1. of the MOU, an "employee" is defined as "a staff employee, contract employee, asset, or other person or entity providing service to or acting on behalf of any agency within the intelligence community."

²³ (U//FOUO) According to paragraph II E. of the MOU, "'Reasonable basis' exists when there are facts and circumstances, either personally known or of which knowledge is acquired from a source believed to be reasonably trustworthy, that would cause a person of reasonable caution to believe that a crime has been, is being, or will be committed."

²⁴ (U//FOUO) Records of the Office of General Counsel indicate there were an average of 200 written crimes reports submitted to DoJ each year for the period 1995-1998.

157. (U//FOUO) In [the] MFR of the OPS Legal Advisor of January 7, 1997, he wrote that another issue discussed was:

The need to determine whether a crimes report will be required after an assessment of the information stored on the drives and the PCMCIA cards. [18 U.S.C. §§ 1924 and 793(f) were briefly discussed.] The General Counsel will make any determination in that regard.

158. (U//FOUO) The OPS Legal Advisor stated that he understood that Deutch had placed classified information on unclassified CIA computers that were connected to the Internet, and the classified information only "came out of Deutch's head" when he composed documents on the computer. The OPS Legal Advisor said he did not know or have any information that Deutch had removed documents from controlled areas containing classified information.²⁵

²⁵ (U//FOUO) Title 18 U.S.C. §§ 793(f) and 1924 both prohibit the improper removal of "documents."

159. (U//FOUO) The OPS Legal Advisor remembered discussing the issue of the possible criminality of Deutch's actions with the PDGC. His position was more conservative than the PDGC's. She raised the point that, as DCI, Deutch had the legal authority to declassify material under his control. This led to her contention that Deutch could not be prosecuted for a security violation. She reportedly cited an instance when then-DCI William Casey inadvertently divulged classified information in an interview with the media.

160. (U//FOUO) The OPS Legal Advisor provided handwritten notes from January 6, 1997 about a discussion of a possible crimes report with the PDGC:

Talked to [the PDGC]. She already knew about the Deutch leak. Discussed the 793(f) issue. She concluded years ago that the DCI who has authority to declassify cannot realistically be punished under the statute. I expressed my disbelief in that analysis. Hypo - does that put the DCI beyond espionage statutes? No she says that would be a natl. security call Returned briefly to information in play. Discussed how there may have been [non-CIA controlled compartmented program material] on the computer. Doesn't this push 793(f) back into play?

161. (U//FOUO) In his OIG interview, the OPS Legal Advisor said that DoD material and Top Secret/ [the non-CIA controlled compartmented program] material would not qualify for information a DCI had the authority to declassify. He realized that a referral to the FBI would "technically not" be the same as making a crimes report to DoJ. He stated there was a tendency to discuss some cases with

the FBI in order to get their procedural advice.

162. (U//FOUO) The OPS Legal Advisor had a discussion with an FBI agent then assigned to the Counterespionage Group, Counterintelligence Center (CIC), regarding the possible applicability of Title 18 U.S.C. §§ 793(f) and 1924 in the matter regarding Deutch. The OPS Legal Advisor recalled this FBI Agent believing that there had to be a physical removal of documents to constitute a violation of the statutes.

163. (U//FOUO) A two-page handwritten note of January 24, 1997, composed by the OPS Legal Advisor, reported his discussion with the FBI Agent regarding the case. The note indicated that the FBI Agent at CIC suggested that it was better to have O'Neil call the then-FBI General Counsel to discuss the case.

164. (U//FOUO) The OPS Legal Advisor provided an MFR reporting a January 28, 1997 meeting with the PDGC and O'Neil to discuss the Deutch case. At that time, O'Neil indicated he

anticipated calling the FBI General Counsel to tell him CIA intended to conduct an investigation of this matter unless the FBI General Counsel wanted the FBI to assert investigative authority.

165. (U//FOUO) According to O'Neil, neither he nor anyone else suggested a crimes report be filed on the Deutch matter. O'Neil said a crimes report can be made at several points during an investigation. He pointed out that, in a number of cases, CIA conducts its own investigation. Matters could also be referred to DoJ to conduct an investigation.

166. (U//FOUO) O'Neil is not certain whether he talked to the FBI agent at CIC about the Deutch matter. O'Neil has a vague recollection he called the FBI General Counsel and asked him how CIA should proceed. O'Neil described the case to the FBI General Counsel, who said that the CIA should continue its own process of looking at the matter. O'Neil believes he wrote an MFR documenting his conversation and may have given the MFR to his secretary to keep in a personal folder used for sensitive matters.²⁶

²⁶ (U//FOUO) A check of O'Neil's "sensitive personal file" was conducted by his secretary's successor in OGC. There was no evidence of any document regarding contact between O'Neil and the FBI General Counsel concerning a possible crimes report on Deutch.

167. (U//FOUO) The FBI Agent at CIC recalled that he was told Deutch had classified information on a computer disk at his home in Maryland shortly after the matter was discovered. The FBI Agent was asked if the matter was an "811" violation.²⁷ The FBI Agent concluded there was no reason to believe that the information had been compromised to a foreign power and, therefore, the FBI did not need to get involved. The FBI Agent recalled telling someone at CIA, whose identity he does not remember, that since Deutch was involved, O'Neil may want to contact the FBI General Counsel, O'Neil's counterpart at FBI. The FBI Agent said that he established early on in his tenure at CIA that merely telling him something did not constitute official notification of the FBI much less DoJ. He was aware that OGC had crimes reporting responsibilities, and he expected them to fulfill those responsibilities.

²⁷ (U) "811" is Section 811 of the Counterintelligence and Security Enhancement Act of 1994.

168. (U//FOUO) The FBI General Counsel recalled a single telephone call from O'Neil after Deutch left CIA, between February and April 1997. At that time, O'Neil told the FBI General Counsel an issue had arisen about classified information existing on some computer disks at Deutch's home. The FBI General Counsel recalled they discussed CIA reporting requirements to the FBI under

"811." [He] believes he would have told O'Neil that not enough was known about the matter at the time. If an "811" problem surfaced after CIA had looked into the matter, CIA should refer the problem to the FBI through official CIA channels.

169. (U//FOUO) The FBI General Counsel stated that he did not consider O'Neil's call as a submission of a crimes report because, from what he remembers being told, there was no evidence of a crime. He said that he and O'Neil spoke on the telephone several times a week, but O'Neil never made a crimes report to him. [He] said that if he thought O'Neil was giving him a crimes report, he would have told him to do it through the proper channel.

170. (U//FOUO) Calder said that if a referral should have been made to DoJ and was not, he believes the omission was not intentional. However, Calder stated the responsibility for a crimes report was O'Neil's. Calder added that "I have never issued a crimes report and would always raise such an issue with OGC for their action." Calder said the FBI General Counsel had informed O'Neil that DoJ would not pursue a Deutch investigation regarding misuse of the computer.

171. (U//FOUO) The PDGC had supervisory responsibility of the Litigation Division which had the crimes reporting account in OGC at that time.²⁸ The PDGC stated she did not have a lot of hands-on experience with the mechanics of coordinating crimes reports and had never authored a crimes report. She first learned of the discovery of classified information, including Top Secret/[a non-CIA controlled compartmented program] material, on a computer in Deutch's Maryland residence on the day of its discovery in December 1996. She remembered hearing about information regarding a covert action with [two countries] but does not recall hearing there was [codeword] or [a different codeword] information on the computer. She did not learn that the computer at his Belmont residence also contained classified information.

²⁸ (U//FOUO) The PDGC has served in the CIA since 1982. (She] was appointed PDGC, the second highest position in the Office of General Counsel, in the summer of 1995 and served in that capacity until March 1, 1999. While serving as PDGC, [she] also served as Acting General Counsel from the August 11, 1997 until November 10, 1997.

172. (U//FOUO) The PDGC was not aware that Deutch was deleting files from the Maryland computer in the days immediately following the discovery of the classified information. She remembered speaking with Calder about the necessity of protecting the magnetic media. Her reason for wanting to retain the magnetic media was not for evidence of a crime but to have a record should there be a need to conduct a leak investigation in the future.

173. (U//FOUO) When considering the need for a crimes report, the PDGC said she did not examine the "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes." She did not consult with any attorneys from the Internal Security Section of DoJ or with the United States Attorneys Office. She does not remember reviewing Title 18 U.S.C. § 793(f), "Gathering, transmitting or losing defense information." She spoke with O'Neil's Executive Assistant²⁹ regarding the provisions of Title 18 and with the OPS Legal Advisor. She did not agree with the OPS Legal Advisor's assertion that, because the classified information "was [only] in his [Deutch's] head," Deutch did not remove classified information from the Agency. The PDGC was aware that, on occasion, Deutch carried the PCMCIA cards "back and forth" with him. She did not know if the cards contained classified information. The PDGC saw no distinction between classified information on a document as opposed to being on magnetic media. She explained that she was more concerned at this time with protecting and recovering the magnetic media than considering a crimes report.

²⁹ (U//FOUO) The then-Executive Assistant to the GC states he was aware of the inquiry regarding the classified information found on Deutch's computer and that it was being worked by others in OGC. The Executive Assistant does not remember assisting the PDGC in this matter, but concludes that, if the PDGC states that he assisted her, he has no reason to doubt her

recollection.

174. (U//FOUO) The PDGC reviewed the statutes she thought would be relevant, and did not see all the elements present for a violation. She believed that Deutch, as DCI, was the authority for the rules concerning the handling of classified information. Because Deutch issued DCIDs on classified material, she believed he could waive the rules for himself. The PDGC recognized that the DCI cannot declassify Top Secret/ [the non-CIA controlled compartmented program] material, but said such material may be handled under the DCID rules. The PDGC stated that given the fact that this matter involved a former DCI, if she had believed a crimes report was necessary, she would have shown the draft to O'Neil and he would have had the final say as to whether a crimes report was warranted.

175. (U//FOUO) The PDGC focused on Title 18 U.S.C. § 1924, "Unauthorized Removal and Retention of Classified Documents or Material." She understood that Deutch was authorized to remove classified information and take it home since he had a safe at his residence. She stated that she did not see "intent"³⁰ by Deutch. She reasoned that "intent" was a necessary element, "otherwise everyone [inadvertently] carrying classified information out of a CIA building would be the subject of a crimes report." According to the PDGC, Deutch had permission to take the classified material home, and Deutch's use of the PCMCIA cards was permissible within his residence. In the PDGC's view, the security violation occurred when he "did not do it right" by connecting the Internet to his computer and "leaving the card in the slot." She did not distinguish between Deutch as DCI and his actual status as an Independent Contractor when the classified information was discovered. However, she would have looked at the issue differently if she understood that the only acceptable means of safeguarding the computer would have been to remove and secure the computer's hard drive.

³⁰ (U) The statute contains the pertinent phrase "and with the intent to retain such documents or materials at an unauthorized location."

176. (U//FOUO) The PDGC did not remember when she made the legal decision that a crimes report was not required. She remembered speaking with C/SIB in March 1997 about his concern that a crimes report should be filed.

177. (U//FOUO) The PDGC said that D/OPS's report was not made available to her. Although someone in OGC would usually read OPS reports, the PDGC speculated that the D/OPS would not have shown the report to her without receiving authorization. She never thought to request a copy of the D/OPS's report to determine if his findings were consistent with her decision not to file a crimes report. Later, after she became Acting General Counsel, the issue of her reviewing the report never arose, and she would have expected OPS to raise the report with her only if the facts had changed significantly from what she learned initially.

178. (U//FOUO) In comparing the Deutch case to a similar case involving a senior Agency official, the PDGC asserted that the other official did not have a safe in his residence and was not authorized to take home classified information. She viewed this dissimilarity as a major distinction. Nor did he have the authority to waive the rules on the handling of classified information. The PDGC did not remember if OGC made a crimes report on that case of mishandling classified information.³¹

³¹ (U//FOUO) A crimes report was made by letter to DoJ on December 13, 1996. It is signed by the AGC in the Litigation Division, who was the OGC focal point for crimes reports at that time.

179. (U//FOUO) George Tenet, who was Acting DCI at the time of the OPS/SIB investigation, said no one ever raised the issue of reporting this incident to DoJ, and it did not occur to him to do so. Tenet said no one ever came forward with a legal judgment that what had occurred was a crime. In Tenet's opinion, based upon what he knew at that time, there was no intent on Deutch's part to

compromise classified information. Therefore, Tenet did not believe a crime was committed. Tenet was aware of the incident involving [another] senior Agency official but was not aware a crimes report had been filed on it.

SHOULD APPLICATION OF THE INDEPENDENT COUNSEL STATUTE HAVE BEEN CONSIDERED?

180. (U) The fundamental purpose of the Independent Counsel statute is to ensure that serious allegations of unlawful conduct by certain federal executive officials are subject to review by counsel independent of any incumbent administration.

181. (U) Title 28 U.S.C. § 592, "Preliminary investigation and application for appointment of an independent counsel" cites Title 28 U.S.C. § 591, "Applicability of provisions of this chapter," as the basis for those positions who are "covered persons" under the Independent Counsel statute.

182. (U) Title 28 U.S.C. § 591 (a), "Preliminary investigations with respect to certain covered persons," specifies:

The Attorney General shall conduct a preliminary investigation in accordance with Section 592 whenever the Attorney General receives information sufficient to constitute grounds to investigate whether any person described in subsection (b) may have violated any Federal criminal law other than a violation classified as a Class B or C misdemeanor or an infraction.³²

³² (U) Title 18 U.S.C. § 793(f) and Title 18 U.S.C. § 798 are felonies; Title 18 U.S.C. § 1924 is a Class A misdemeanor.

183. (U) Title 28 U.S.C. § 591 (b), "Persons to whom subsection (a) applies" lists:

... the Director of Central Intelligence [and] the Deputy Director of Central Intelligence³³

³³ (U) Title 28 U.S.C § 591(b)(7) limits applicability of the statute to the term of office of the "covered person" and the one-year period after the individual leaves the office or position. This means that Deutch's potential exposure to the provisions of the Independent Counsel statute expired following the one-year anniversary of his resignation, December 14, 1997.

184. (U) Title 28 U.S.C. § 591 (d) (1), "Examination of information to determine need for preliminary investigation," "factors to be considered" specifies:

In determining ... whether grounds to investigate exist, the Attorney General shall consider only -- (A) the specificity of the information received; and (B) the credibility of the source of the information.

185. (U) The Deputy Chief, Public Integrity Section, Criminal Division, DoJ, is responsible for the preliminary review of matters referred to DoJ under the provisions of the Independent Counsel statute. [She] explained that the provisions of the Independent Counsel statute require DoJ to review an allegation regarding a "covered person" to determine the need for preliminary investigation based only on the two factors listed above.

186. (U/ /FOUO) The Deputy Chief of the Public Integrity Section explained that after the CIA IG referral in March 1998, the Public Integrity Section reviewed the matter and described it in a memorandum to the Attorney General. The memorandum stated that the allegations of illegal behavior regarding former DCI Deutch were received more than one year after Deutch left office.

Accordingly, under the provisions of the Independent Counsel statute, Deutch was no longer a "covered person." The Deputy Chief of the Public Integrity Section added that the allegation should have been promptly referred to DoJ by CIA personnel.

187. (U//FOUO) The OPS Legal Advisor stated that he never considered the need to refer this matter to an Independent Counsel based on Deutch's status as a "covered person." Nor was he aware of any other discussions on this matter.

188. (U//FOUO) The PDGC stated that the issue of Deutch being a "covered person" under the Independent Counsel legislation did not arise. She said that "she never gave a thought," to the applicability of the Independent Counsel statute, and she does not know what positions within the Agency are specified as "covered persons."

189. (U//FOUO) O'Neil stated that there was no recommendation to refer the Deutch matter to DoJ under the provisions of the Independent Counsel statute.

WERE SENIOR AGENCY OFFICIALS OBLIGATED TO NOTIFY THE CONGRESSIONAL OVERSIGHT COMMITTEES OR THE INTELLIGENCE OVERSIGHT BOARD OF THE PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD? WERE THESE ENTITIES NOTIFIED?

190. (U) Pursuant to the National Security Act of 1947, as amended, the President and the DCI bear statutory responsibility for keeping the two Congressional intelligence committees *fully and currently* informed of all intelligence activities.

191. (U//FOUO) Agency Regulation (AR) 7-2, "Reporting of Intelligence Activities to Congress," provides interpretation of the statutes so the Agency, with the assistance of the Office of Congressional Affairs and the Office of General Counsel, can assist the DCI in meeting the obligation to keep the intelligence committees fully and currently informed. Under the section, "Obligation to Keep Congressional Intelligence Committees Fully and Currently Informed," one of the three categories requiring reporting are:

Particular intelligence activities or categories of activities as to which either of the Congressional intelligence committees has expressed a continuing interest (for example, potentially serious violations of U.S. criminal law by Agency employees, sources, or contacts);

192. (U) E.O. 12863, issued September 13, 1993, President's Foreign Intelligence Advisory Board, specifies:

The heads of departments and agencies of the Intelligence Community, to the extent permitted by law, shall provide the Intelligence Oversight Board (IOB) ³⁴ with all information that the IOB deems necessary to carry out its responsibilities. Inspectors General and General Counsel of the Intelligence Community, to the extent permitted by law, shall report to the IOB, at least on a quarterly basis and from time to time as necessary or appropriate, concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive.

³⁴ (U) The Intelligence Oversight Board is a standing committee of the President's Foreign Intelligence Advisory Board.

193. (U//FOUO) According to the Director of the CIA's Office of Congressional Affairs (OCA), OCA is responsible for notifications to Congress and should be informed of any formal Agency investigations. OCA receives notifications from a variety of Agency components. During Slatkin's tenure, all formal written Congressional notifications were to be routed through her office. The

Director of OCA was unaware of SIB's investigation into the discovery of classified information on Deutch's government-issued unclassified computer.

194. (U//FOUO) At the January 6, 1997 meeting to discuss the planned investigation of the finding of classified information on Deutch's unclassified CIA computer, the OPS Legal Advisor stated that the Congressional oversight committees may eventually inquire about this matter. He recalled that Calder wanted the investigation performed "by the book" in case there would be a need to account for SIB actions.

195. (U//FOUO) Calder assumed this matter would again arise in the future, possibly through a leak, with a Congressional committee. He recalled a discussion about doing briefings and was left with the impression that there was a briefing of the "Group of Four" Congressional oversight committees.³⁵

³⁵ (U) The Group of Four refers to the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, and the two appropriations committees-- the Senate Appropriations Committee, Subcommittee on Defense and the House Appropriations Committee, National Security Subcommittee.

196. (U//FOUO) C/SIB maintained a chronology of the investigation consistent with Calder's instructions. He also advised Calder, the former ADDA, the PDGC, and the D/OPS on at least two occasions that Congress, along with DoD, should be informed about the material found on Deutch's unclassified computer. After receiving a copy of the D/OPS's report on the investigation, C/SIB realized the report did not contain a recommendation that Congress be notified.

197. (U//FOUO) The PDGC stated she did not remember any discussion concerning notifying the Congressional oversight committees or the IOB. O'Neil said that "the question of informing the IOB or the Congressional oversight committees did not come up."

198. (U//FOUO) Slatkin stated she could not recall any discussion or recommendation regarding the need to notify the Congressional committees about the Deutch matter. In her interview with OIG, she stated that, "surely, yes, the Committees should have been notified--but at what point?"

199. (U//FOUO) The IOB was officially notified of OIG's investigation on May 8, 1998. After being informed of the OIG investigation, the Director of Congressional Affairs prepared talking points, which DCI Tenet presented to the SSCI and HPSCI in early June 1998.

WHY WAS NO ADMINISTRATIVE SANCTION IMPOSED ON DEUTCH?

200. (U//FOUO) Deutch was aware that an inquiry was conducted after classified information was discovered on his government-issued computers configured for unclassified use. He said that he never tried to influence the outcome of the investigation. Nor was he told the outcome, although he had requested that someone apprise him of the results.

201. (U//FOUO) Calder said that, despite the pressure that accompanied the investigation of a DCI, he and OPS did "the right thing." Calder said that since Deutch was no longer a CIA employee, there was no punishment that could be administered to him. The issue was what position the Agency should take if Deutch needed access to classified information in the future. Calder was aware that Deutch's computers had been replaced with totally unclassified magnetic media. Calder said that while Deutch was on several governmental committees, he did not believe that Deutch had a need for classified information in those positions. Calder said the remedy was to counsel Deutch in a discrete manner that would not offend his ego so he would understand the gravity of what had happened. Calder was aware that Slatkin had spoken with Deutch about the issue, and, from those conversations, Deutch would have recognized that his actions were wrong. Calder stated it was his responsibility to counsel Deutch and he planned to do so when Deutch received a briefing regarding future access. However,

Calder said he never had the opportunity to meet with Deutch under the conditions he desired.

202. (U//FOUO) The former ADDA stated that she was "worn down" by Slatkin and O'Neil, and perceived that the D/OPS and Calder were similarly affected. Additionally, Calder was "frustrated" because Slatkin would not resolve issues presented to her but, instead, provided more tasking. The former ADDA said that she, the D/OPS, and Calder had reached a point where they could not go any further in that there was no additional merit in further evaluating the collected data. Slatkin had "emotional attachments" and O'Neil was not considered to be objective. According to the former ADDA, Slatkin's and O'Neil's oversight of the investigation was colored by a distrust of OPS and an interest to protect Deutch's privacy. The former ADDA said that she and SIB investigators perceived Slatkin's and O'Neil's behavior as "stonewalling." The former ADDA and SIB investigators also viewed Slatkin's requests for repeated clarifications, while typical of her management style, as a form of "pressure" to wear down the others until they were ultimately in agreement with her and O'Neil.

203. (U//FOUO) The PDGC said that there was not a "crisp end" to the case; "it ran out of steam" when many of the principals left the Agency. The PDGC thought a decision was made that the Director of the Center for CIA Security or the D/OPS would brief either Deutch or the whole Proliferation Commission regarding safeguarding classified information, but she does not know if this action was taken. O'Neil stated that after the process for producing the review was approved by the ADCI, who had been kept informed all long, he had little to do with the investigation. O'Neil also stated, he did not interfere with the OPS investigation, he left the Agency in July 1997,³⁶ and he does not know how the investigation was concluded. Slatkin said that she gave the information to Tenet and assumed that the investigation would have proceeded after she departed the Agency. The D/OPS said that, as far as he knows, no decision was ever made on what to do concerning Deutch's actions.

³⁶ (U//FOUO) Although O'Neil states he left the Agency in July 1997, he was present for duty until August 11, 1997 when he was replaced by the PDGC as Acting General Counsel.

204. (U//FOUO) Tenet did not recall how the matter was resolved. He believes Calder, the D/OPS, Slatkin, and O'Neil had detailed discussions on the matter. Tenet was aware of concerns for Deutch's privacy. According to Tenet no one ever raised the issue of reporting the incident to the Department of Justice, or whether Deutch's clearance should be affected.

WHAT WAS OIG'S INVOLVEMENT IN THIS CASE?

- **When did OIG first learn of this incident?**

205. (U//FOUO) The former C/DCI Administration spoke with then-IG Frederick Hitz on December 18, 1996³⁷ regarding what was found at Deutch's residence. The former C/DCI Administration described conversations he had with O'Neil and Slatkin about the matter, and O'Neil's assertion that the former C/DCI Administration was responsible for allowing Deutch to improperly process classified information. Hitz instructed the former C/DCI Administration to provide the IG with copies of any documentation,³⁸ encouraged the former C/DCI Administration to brief Tenet as soon as possible, and suggested that the former C/DCI Administration stay in contact with the IG.

³⁷ (U//FOUO) Hitz served as CIA IG from October 12, 1990 until April 30, 1998, when he retired.

³⁸ (U//FOUO) The former C/DCI Administration provided a copy of his MFR to Hitz, Calder, and C/SIB.

206. (U//FOUO) According to the former C/DCI Administration's MFR of December 30, 1996, the IG Counsel contacted him on December 19, 1996. Reportedly, the IG Counsel urged the former

C/DCI Administration to prepare an MFR and provide related documentation to the IG.

207. (U//FOUO) On December 20, 1996, Hitz called the former C/DCI Administration to inform him that he had met with Tenet, who was reportedly not aware of the Deutch matter. Hitz indicated that he and Tenet both supported the process that was being pursued on the acquisition of relevant information and the classified magnetic media. Hitz encouraged the former C/DCI Administration to ensure that his documentation was forwarded to Hitz's staff for the former C/DCI Administration's protection.

208. (C) Hitz remembers that in mid-December 1996, the former C/DCI Administration met with him regarding classified information discovered on one or two Agency-owned computers at Deutch's residences in Maryland and Belmont. Hitz recalled the former C/DCI Administration seeking advice on what action to take. Hitz's impression was that C/DCI Administration was concerned that the former C/DCI Administration's supervisors would not act appropriately. Hitz understood that the classified information found on Deutch's computer included sensitive trip reports. The computer was connected to the Internet, and there was [a] threat of the information being vulnerable to electronic compromise.

209. (U//FOUO) Hitz believes that he discussed the former C/DCI Administration's information with IG Counsel and the then-Deputy IG for Investigations and obtained their advice. This advice included instructing the former C/DCI Administration to secure the hard drive and other classified information that was recovered from Deutch's computers. Hitz remembered passing that instruction to the former C/DCI Administration. Hitz recalled that after meeting with IG Counsel and then-Deputy IG for Investigations, "we knew we were going to get into it and be helpful with it."

210. (U//FOUO) Hitz stated that he cannot remember what follow-up instruction he may have provided to IG Counsel and then-Deputy IG for Investigations. Hitz thinks he ultimately read the former C/DCI Administration's MFR and "did not like the smell of it" [the nature of the allegation] and "if half of what the former C/DCI Administration said was true - we would get in it." Hitz emphasized that the determination of whether to get involved would be made in concert with IG Counsel and the then-Deputy IG for Investigations. Hitz stated he never discussed the SIB investigation with Deutch, Slatkin, O'Neil, Calder, the PDGC, or D/OPS.

211. (U//FOUO) IG Counsel said that he does not remember any discussions that Hitz may have had with him and the then Deputy IG for Investigations stemming from information received from the former C/DCI Administration. The IG Counsel stated that he does not remember calling the former C/DCI Administration or having any discussion of an allegation regarding Deutch, nor does he remember seeing an MFR by the former C/DCI Administration.³⁹

³⁹ (U//FOUO) A review of Hitz's files, which he left when he retired, failed to locate [the] MFR of the former C/DCI Administration or any notes or correspondence connected with this investigation.

212. (U//FOUO) The then-Deputy IG for Investigations said there were contacts between the former C/DCI Administration and Hitz over this issue, and Hitz would tell the then-Deputy IG for Investigations about the conversations afterwards. The then-Deputy IG for Investigations stated he "may have detected an inference from Hitz that classified information was on the computer." However, the then-Deputy IG for Investigations did not remember any discussion with Hitz regarding the need to protect the computer's hard drive. The then-Deputy IG for Investigations was not in contact with the former C/DCI Administration.

- **Why did OIG wait until March 1998 to open an investigation?**

213. (U//FOUO) Hitz observed that the investigation had started with the former C/DCI

Administration's "security people" finding the data, and the investigation stayed in a security channel. Hitz believed that it was appropriate for that to continue as long as OPS would be allowed to do their job.

214. (U//FOUO) C/SIB's chronology noted a call from the then-Deputy IG for Investigations on January 7, 1997 asking that SIB look at a particular issue, normally the purview of the OIG (improper personal use of a government computer) to put some preliminary perspective to the issue and keep him apprised.

215. (U//FOUO) The then-Deputy IG for Investigations stated that he must have learned from Hitz that C/SIB was involved with an investigation related to Deutch and that knowledge prompted the then-Deputy IG for Investigations to call C/SIB on January 7, 1997. The then-Deputy IG for Investigations said that, if he had been informed that the matter under investigation by C/SIB was a "serious issue," he would remember it. The then-Deputy IG for Investigations categorized the issue under investigation by SIB as one of "propriety and property management." He does not recall knowing that the computers involved were intended for unclassified use.

216. (U//FOUO) The OPS Legal Advisor stated he learned from Calder that on January 5, 1997, Hitz was briefed on the incident involving Deutch. Reportedly, Calder stated that Hitz believed that the incident was a security issue and not one for the IG. After learning of Deutch's possible appointment to the Office of Science and Technology Policy, on May 16, 1997, [the OPS Legal Advisor] wrote in an MFR that he met briefly with Hitz to discuss Deutch's possible appointment and Fred [Hitz] said he would speak to the DCI about this matter, and sensitize him to the problems associated with [Deutch's] needing a clearance at another U.S.G. agency. Fred asked to be kept informed. ⁴⁰

⁴⁰ (U//FOUO) Hitz corroborates the OPS Legal Advisor's account of this meeting.

217. (U//FOUO) According to C/SIB, he contacted OIG to define OIG interests before the D/OPS began his review of the recovered documents. C/SIB met with the then-Deputy IG for Investigations, the IG Counsel, and the then-Deputy Associate IG for Investigations. C/SIB advised them that any difficulties he encountered to date were within his ability to resolve. In his chronology, C/SIB writes:

C/SIB met with [the then-Deputy IG for Investigations, the Deputy Associate IG for Investigations and the IG Counsel] re "reporting threshold" to OIG for USG Computer Misuse, both in this case in particular, and in other cases, in general. This meeting was imperative in order for C/SIB to know before the "security" review [being conducted by [the] D/OPS] what would vice would not be OIG reportable. Upon discussion, it was determined that the OIG would avail great latitude to SIB re such reporting, noting that only in instances wherein the use of the computer was obviously criminal in nature, a conflict of interests [sic] existed, an outside business was being conducted, or a private billing reimbursement for "personal entertainment" was in evidence, would the OIG require a report be submitted by SIB. (C/SIB so advised D/OPS). No particulars ⁴¹ were discussed relative to SIB's ongoing investigation, nor were any requested.

⁴¹ (U//FOUO) C/SIB later explains his use of the word "particulars" meant that he did not disclose what evidence had been discovered in his investigation. He states that it does not necessarily mean that Deutch's name and/or title was not discussed.

218. (U//FOUO) The then-Deputy IG for Investigations remembers the February 21, 1997 meeting with C/SIB in the presence of the Deputy Associate IG for Investigations, and possibly the IGCounsel. Up to that point, OIG had lost track of the allegation against Deutch. The then-Deputy IG for Investigations stated he told C/SIB about OIG's jurisdictional interests in terms of the computer. The then-Deputy IG for Investigations said it is possible that C/SIB made some comment about encountering some difficulty in the investigation but was working through the problem and appeared

self-confident about his capability to investigate the matter. The then-Deputy IG for Investigations sensed that C/SIB was being "squeezed by unspecified OPS officials."

219. (U//FOUO) The then-Deputy IG for Investigations remembered C/SIB agreeing that he should re-contact OIG if he encountered any matter of IG interest, such as evidence of misuse of an official computer, during his investigation. According to the then-Deputy IG for Investigations, "there was no zest" on the part of OIG to take it over while OPS was working the issue. The then-Deputy IG for Investigations does not recall knowing at the time that the OPS/SIB investigation involved classified information.

220. (U//FOUO) On February 6, 1998, the Deputy Associate IG for Investigations met with C/SIB on an unrelated investigation. C/SIB incorrectly assumed the Deputy Associate IG for Investigations was investigating Deutch's mishandling of classified information on a computer at his residence. According to the Deputy Associate IG for Investigations, C/SIB disclosed that he was unable to fully pursue his investigation because of a problem with Slatkin and O'Neil. C/SIB was frustrated because there had been no interview of Deutch, a customary part of an SIB investigation.

221. (U//FOUO) During this meeting, the Deputy Associate IG for Investigations reviewed a number of documents that included an unsigned report prepared by the D/OPS. This report detailed the D/OPS review of data discovered on the Deutch's magnetic media. The Deputy Associate IG for Investigations, subsequently met with the then-Deputy IG for Investigations, and told him what he had learned from C/SIB.

222. (U//FOUO) In his OIG interview, the then-Deputy IG for Investigations explained that OIG opened an investigation because SIB's investigation was impeded or "shutdown," and a crimes report was never sent to DoJ.

223. (U//FOUO) Hitz explained that a security violation of this nature would not normally be a matter investigated by OIG.⁴² He stated that as the IG, he would have been inclined to assert investigative authority only when he believed that the normal management response was inappropriate or not helpful. He recognized that Deutch appointees Slatkin and O'Neil were involved in the review process. Hitz stated that it was the responsibility of OIG "to support the institution."

⁴² (U//FOUO) On February 5, 1997, Hitz sent a memorandum to the Director of Personnel Security, Subject: "Crimes Reporting and Other Referrals by Office of Personnel Security to the Office of Inspector General." The memorandum eliminated the requirement for OPS to routinely notify OIG of certain specific investigative matters in which it is engaged. Included as one of the nine categories of investigative issues identified in the memorandum was the following: "Mishandling of classified information that is or could be a possible violation of 18 U.S.C. 1924, 'Unauthorized removal and retention of classified documents or material'."

- **What steps were taken by OIG after opening its investigation?**

224. (U//FOUO) IG Counsel remembered advising the Deputy Associate IG for Investigations that the allegation had to be referred to DoJ as a possible crimes report. The IG Counsel also remembers a discussion about the relevance of the Independent Counsel statute since Deutch was a "covered person."

225. (U//FOUO) On March 19, 1998, OIG referred the allegations to DoJ. The crimes report letter noted that at the time of the alleged violations, Deutch was a "covered person" under the Independent Counsel statute. DoJ advised they would review the allegations for applicability to the Independent Counsel statute and further OIG investigation was not authorized until completion of DoJ's review. In May 1998, DoJ informed OIG that the Independent Counsel statute would not apply because DoJ was not notified of the alleged violations until more than one year after Deutch left his position. As such,

Deutch's status as a "covered person" had expired.

226. (U//FOUO) On May 8, 1998, OIG informed the Chairman of the Intelligence Oversight Board by letter of the criminal investigation of Deutch pursuant to E.O. 12863.

227. (U//FOUO) On June 2 and 3, 1998, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence were notified by DCI Tenet that the OIG was conducting an investigation of former DCI Deutch and the manner in which the matter was originally handled by CIA officials.

WHAT IS DEUTCH'S CURRENT STATUS WITH THE CIA?

228. (U//FOUO) Deutch's no-fee, December 1996 consulting contract was renewed in January 1998 and December 1998. The latest renewal covers the period December 16, 1998 until December 15, 1999. This contract provides Deutch with staff-like access to the Agency, its computer system, and a Top Secret clearance. Deutch's contract for the Proliferation Commission will expire when the commission finishes its work. That contract does not contain any information regarding access to classified information.

WHAT WAS THE DISPOSITION OF OIG'S CRIMES REPORT TO THE DEPARTMENT OF JUSTICE?

229. (U//FOUO) On April 14, 1999, Attorney General Janet Reno sent a letter to DCI Tenet [declining prosecution.] [The letter stated in part:]

The results of that [OIG] investigation have been reviewed for prosecutive merit and that prosecution has been declined. As I understand that Mr. Deutch currently holds a Top Secret security clearance, I suggest that the appropriate security officials at the Central Intelligence Agency review the results of this investigation to determine Mr. Deutch's continued suitability for access to national security information.

CONCLUSIONS

230. (U//FOUO) Former DCI John Deutch was specifically informed that he was not authorized to process classified information on government computers configured for unclassified use.

231. (U//FOUO) Throughout his tenure as DCI, Deutch intentionally processed on those computers large volumes of highly classified information to include Top Secret Codeword material.

232. (U//FOUO) Because Deutch's computers configured for unclassified use had connections to the Internet, all classified information on those computers was at risk of compromise. Whether any of the information was stolen or compromised remains unknown.

233. (U//FOUO) On August 1, 1995, Deutch was made aware that computers with Internet connectivity were vulnerable to attack. Despite this knowledge, Deutch continued his practice of processing highly classified material on unclassified computers connected to the Internet.

234. (U//FOUO) Information developed during this investigation supports the conclusion that Deutch knew classified information remained on the hard drives of his computers even after he saved text to external storage devices and deleted the information.

235. (U//FOUO) Deutch misused U.S. Government computers by making extensive personal use of them. Further, he took no steps to restrict unauthorized persons from using government computers located at his residences.

236. (U//FOUO) The normal process for determining Deutch's continued suitability for access to classified information, to include placing the results of the SIB investigation in Deutch's security file, was not followed in this case, and no alternative process was utilized. The standards that the Agency applies to other employees' and contractors' ability to access classified information were not applied in this case.

237. (U//FOUO) Because there was a reasonable basis to believe that Deutch's mishandling of classified information violated the standards prescribed by the applicable crimes reporting statute, Executive Order and Memorandum of Understanding, OGC officials Michael O'Neil and the PDGC should have submitted a crimes report to the Department of Justice.

238. (U//FOUO) The actions of former Executive Director Nora Slatkin and former General Counsel Michael O'Neil had the effect of delaying a prompt and thorough investigation of this matter.

239. (U//FOUO) DDA Richard Calder should have ensured the completion of a more thorough investigation, in particular, by arranging for an interview of Deutch and a subsequent documentation of that interview in accordance with established Agency procedures. Calder should also have ensured that the matter was brought to a conclusion rather than permitting it to languish unresolved.

240. (U//FOUO) Former Inspector General Frederick Hitz should have involved himself more forcefully to ascertain whether the Deutch matter raised issues for the Office of the Inspector General as well as to ensure the timely and definitive resolution of the matter.

241. (U//FOUO) DCI George Tenet should have involved himself more forcefully to ensure a proper resolution of this matter.

242. (U//FOUO) The application of the Independent Counsel statute was not adequately considered by CIA officials and, given the failure to report to DoJ on a timely basis, this in effect avoided the potential application of the statute.

243. (U//FOUO) The Congressional oversight committees and the Intelligence Oversight Board should have been promptly notified of Deutch's improper handling of classified information.

Daniel S. Seikaly

RECOMMENDATIONS

1. (U//FOUO) John Deutch's continued suitability for access to classified information should be reviewed immediately.

2. (U//FOUO) The accountability of current and former Agency officials, including Deutch, for their actions and performance in connection with this matter should be determined by an appropriate panel.

3. (U//FOUO) All appropriate Agency and Intelligence Community components should be informed in writing of the sensitive information Deutch stored in his unclassified computers so that responsible authorities can take any actions that would minimize damage from possible compromise of those materials.

CONCUR:

L. Britt Snider
Inspector General

Date

COPY

UNITED STATES DISTRICT COURT

for the
Eastern District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)ONE PANASONIC LAPTOP COMPUTER,
TWO WESTERN DIGITAL HARD DRIVES, and
TWO SANDISK CRUZER USB DRIVES

Case No. 1:13sw

274

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.**YOU ARE COMMANDED** to execute this warrant on or before April 18, 2013

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Ivan D. Davis

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.Date and time issued: 4 Apr 13 @ 1536 hrsIvan D. Davis /s/ Ivan D. Davis
Judge's signatureCity and state: Alexandria, VirginiaUnited States Magistrate Judge
The Honorable Ivan D. Davis
Printed name and title

ATTACHMENT A

Property To Be Searched

The property to be searched is as follows:

- One Panasonic Toughbook laptop computer, model number CF-F9KWHZZ1M, serial number 0LKSA22428, hereinafter "the Device."
- Two Western Digital external hard drives, both black in color, bearing serial numbers WXN1098Y4486 and WXN208N10851, hereinafter "the External Hard Drives."
- Two Sandisk Cruzer 4 Gigabyte USB Drives, bearing serial numbers BH1003OCXB and BH1003OBWB, hereinafter "the USB Drives."

The Device, the External Hard Drives, and the USB Drives are currently located in evidence storage in the Office of Inspector General, Central Intelligence Agency, Headquarters Building, Langley, Virginia.

This warrant authorizes the forensic examination of the Device, the External Hard Drives, and the USB Drives for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things To Be Seized

All records or information on the Device, the External Hard Drives, and the USB Drives described in Attachment A that relate to violations of: (a) Title 18, United States Code, Section 1924; (b) Title 18, United States Code, Section 793(e); and (c) Title 18, United States Code, Section 371, including:

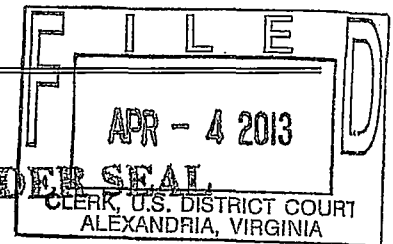
1. All records or information related to any communications between PETRAEUS and [REDACTED];
2. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;
3. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
4. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED];
5. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
6. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

7. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;
8. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS;
9. Any information recording PETRAEUS's schedule or travel from December 2008 to the present;
10. Evidence of user attribution showing who used or owned the Device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, address books, contact lists, saved usernames and passwords, documents, and browsing history; and
11. Records evidencing the use of the Internet, including:
 - i. records of Internet Protocol addresses used;
 - ii. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of social networking and online service usage, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

7. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

ONE PANASONIC LAPTOP COMPUTER,
TWO WESTERN DIGITAL HARD DRIVES, and
TWO SANDISK CRUZER USB DRIVES

Case No. 1:13sw

274

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

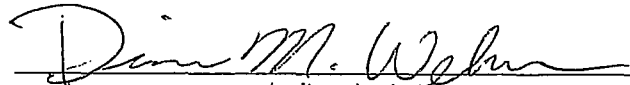
Code Section

Offense Description

18 USC 1924; 18 USC 793(e); 18 USC 371 Unlawful removal and retention of classified documents; unlawful possession and communication of national defense information; conspiracy

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

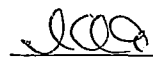

Applicant's signature

Diane M. Wehner, Special Agent, FBI

Printed name and title

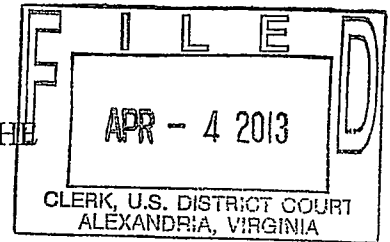
Sworn to before me and signed in my presence.

Date: 04/04/2013City and state: Alexandria, Virginia

 /s/
Ivan D. Davis
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF)
ONE PANASONIC LAPTOP COMPUTER,)
TWO WESTERN DIGITAL HARD DRIVES, and)
TWO SANDISK CRUZER USB DRIVES)

UNDER SEAL

Case No. 1:13sw 274

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, DIANE M. WEHNER, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search both a government laptop computer used by DAVID PETRAEUS and associated external hard drives and USB drives associated with the same government laptop computer. The specifics of the laptop computer and external hard drives and USB drives to be searched and items to be seized are more fully described in Attachments A and B, which are incorporated fully by reference herein.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for approximately seven years. I have investigated matters involving complex financial fraud, public corruption, and counterterrorism. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by individuals attempting to conceal their illegal behavior. I have also received specialized training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government

officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.
5. For the reasons set forth below, there is probable cause to believe that the government laptop computer used by PETRAEUS and the associated external hard drives and USB drives (all described in detail in Attachment A) contain evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful communication and/or retention of classified information.
6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.
9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause “damage” to the national security, the information is classified as “Confidential.” Where such unauthorized disclosure reasonably could be expected to cause “serious damage” to the national security, the information is classified as “Secret.” Where such unauthorized disclosure reasonably could be expected to cause “exceptionally grave damage” to the national security, the information is classified as “Top Secret.”

10. E.O. 13526 also provides that certain senior U.S. officials are authorized to establish “special access programs” upon a finding that “the vulnerability of, or threat to, specific information is exceptional” and “the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.” Within the U.S. Intelligence Community, the Director of National Intelligence is authorized to establish special access programs for intelligence sources, methods, and activities. Such intelligence programs are called “Sensitive Compartmented Information Programs” or SCI Programs.
11. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head’s designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

12. PETRAEUS is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about July 4, 2010 to July 18, 2011, PETRAEUS served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, PETRAEUS served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, PETRAEUS held a United States government security clearance allowing him access to classified United States government information. According to a Department of Defense (DOD) official, to obtain that clearance, PETRAEUS was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled

to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

13. [REDACTED] is a researcher and author of a biography of PETRAEUS, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. According to a DOD official, to obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

14. In 2012, [REDACTED] was the subject of an FBI Tampa Division (FBI Tampa) computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1. This complaint alleged the receipt of threatening and harassing emails from an unknown individual. Witness 1 claimed to have friendships with several high-ranking public and military officials.

15. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of PETRAEUS, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified PETRAEUS's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that PETRAEUS

personally requested that Witness 1 withdraw his/her complaint and “call off the G-men.”

On August 13, 2012, Witness 1 advised FBI Tampa that PETRAEUS believed the alleged cyber stalker possessed information which could “embarrass” PETRAEUS and other public officials. Ultimately the FBI determined, based upon the investigation, that [REDACTED] was the individual who had sent the emails to Witness 1.

16. On September 24, 2012 as part of the FBI Tampa investigation, [REDACTED] consented to a search of two laptops and two external hard drives belonging to her. A review of the digital media contained on these devices revealed over 100 items which were identified by FBI Charlotte Computer Analysis Response Team (CART) Forensic Examiners as potentially containing classified information, up to the Secret level.
17. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with [REDACTED]. He denied providing any classified documents to [REDACTED] or having any arrangement to provide her with classified information. PETRAEUS stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted “off-the-record” access to classified presentations, such as the COMISAF’s (Commander, International Security Assistance Force) daily briefings.
18. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her

time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from PETRAEUS.

19. During interviews conducted of [REDACTED] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of pre-paid cellular telephones and email accounts using non-attributable names. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if all the accounts were identified because both [REDACTED] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [REDACTED]'s September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

20. On November 12, 2012, Agents from the Charlotte and Tampa Divisions of the FBI participated in a consensual search of [REDACTED]'s residence in Charlotte, North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital

media as well as four boxes and one folder of documents. On this same date,

██████████'s administrative assistant voluntarily provided the FBI with digital media as well as one box of documents which she maintained in her home in relation to her employment with ██████████. A review of the seized materials has identified to date hundreds of potentially classified documents, including more than 300 marked Secret, on digital images maintained on various pieces of electronic media.

21. Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. ██████████ traveled into and out of Afghanistan several times between September 2010 and July 2011 to conduct research for a biography on PETRAEUS. During this time, PETRAEUS was serving as the International Security Assistance Force (ISAF) Commander.
22. ██████████'s paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting ██████████ access to classified information for the purpose of writing his biography. For example, in an email dated January 16, 2011, which Petraeus marked as CONFIDENTIAL and sent to multiple members of the military, he instructed a member of his staff to "PLS PRINT FOR ██████████, ON AN OFF THE RECORD BASIS." Travel documents show that ██████████ was in Afghanistan at this time.

A. Communications Regarding Potential Mishandling of Classified Information

23. On May 12, 2011, ██████████, using email account ██████████, sent an email to PETRAEUS at email account ██████████. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training,

experience, and information reviewed to date in this investigation, your affiant believes the email related to a document or series of documents provided by PETRAEUS to [REDACTED] which contained classified information.

24. Between July 13, 2011 and July 15, 2011, [REDACTED] and a [REDACTED] Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED], emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED] on July 15, 2011, he advised he was working on the storyboards and asked her for "a good SIPR number."¹ Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) PETRAEUS at email account [REDACTED]. [REDACTED]'s response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel likely reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

25. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED], and PETRAEUS, using email address [REDACTED]

¹ SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

[REDACTED], discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which PETRAEUS addressed by typing in all capital letters within the body of [REDACTED]'s original emails. In the email string, while discussing PETRAEUS's files, [REDACTED] wrote, "[T]he [REDACTED] letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED]'s email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

26. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED] [REDACTED], the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there."² In response PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

27. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address [REDACTED], and [REDACTED], using email address [REDACTED], exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "[REDACTED] files" as well as other files and expressed his willingness to share them with [REDACTED]. PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about PETRAEUS's

² NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

willingness to share the files writing: “[I]’ll protect them. And I’ll protect you.”

PETRAEUS later responded to [REDACTED], writing, “[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they’re upstairs, but they’re not organized enough at this point...”³ PETRAEUS continued, writing, “[A]nd I think MNSTC-I files went to NDU, though I’m not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class’d, but I guess I might share!**” (emphasis added).

28. Your affiant believes that PETRAEUS’s reference to “Class’d” means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified.

B. Audio Recordings Indicating Potential Mishandling of Classified Information

29. PETRAEUS, in his capacity as ISAF Commander, maintained a digital recorder and may have used the recorder to capture select conversations. Your affiant has identified at least five images on the internet which show PETRAEUS with a recorder. One image shows PETRAEUS in military uniform, apparently in Afghanistan, another is a photograph from [REDACTED]’s Facebook account showing PETRAEUS and [REDACTED] sitting together in an office, believed to be [REDACTED]’s office in Afghanistan. Your affiant has reviewed audio files recovered from [REDACTED]’s digital media and identified recorded conversations in which [REDACTED] is not heard on the recording and is not

³ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). PETRAEUS was the former commander of MNF-I.

believed to have been present. Based upon the content of these recordings, your affiant believes the recorded conversations were originated by PETRAEUS. Your affiant has reviewed publicly available video and audio voice files of PETRAEUS and believes that the above-referenced recordings do include the voice of PETRAEUS. Investigators have not yet recovered any digital recorders from [REDACTED] or PETRAEUS.

30. In an audio file located on a computer received from [REDACTED]'s administrative assistant, there is a recording of an interview conducted by [REDACTED] during the course of her research on PETRAEUS. This recording is approximately twenty-four minutes, and based on the content of the audio, seems to have been recorded in the August 2011 timeframe. During the recorded conversation, [REDACTED] informed an unknown individual she was interviewing that she would be traveling to Washington, D.C. a lot that month to meet with PETRAEUS and would go through boxes in "his attic."

31. In an audio file located on a hard drive seized from [REDACTED]'s residence on November 12, 2012, there is a recorded conversation between PETRAEUS and, inter alia, Washington Post reporters, which, based on the information and belief of your affiant, occurred in or about March 2011. In the conversation, PETRAEUS stated, "[I] would really love to be on background as a senior military officer." Later in the recording, PETRAEUS discusses sensitive military campaigns and operations, some of which, on the basis of a preliminary review by another government agency designated to assist in this investigation, is believed to contain classified information, including information at the Top Secret level.

32. In an audio file located on electronic evidence seized from [REDACTED]'s residence on November 12, 2012, there is a recorded conversation between PETRAEUS, a reporter, and at least one other individual. During the conversation, PETRAEUS requested that information he provided be attributed to a "defense official familiar with PETRAEUS's activities." PETRAEUS was concerned about the sensitivity of the information he was providing, and wanted to ensure the information was not attributed to him because it would come out after he was confirmed as Director of the CIA. PETRAEUS then discussed with the reporter information that, on the basis of a preliminary review by another government agency designated to assist in this investigation, is believed to be classified, including information at the Top Secret level.

C. Additional Evidence of Potential Mishandling of Classified Information

33. In an email dated June 26, 2011, an Army historian previously assigned to ISAF replied to an email from PETRAEUS in which PETRAEUS discussed [REDACTED]'s research efforts. In the body of the Army historian's response, the historian wrote, "I [am] happy to receive [REDACTED]'s research effort and will add it to the collection. It is still my understanding that your 'black books' and other sensitive items are off limits. She can look at the other documents such as update briefs, info papers, photos, and other reference materials, but not the sensitive ones. Am I correct on that rule?"

34. In an audio file located on a laptop computer seized from [REDACTED], there is a recorded conversation between [REDACTED] and PETRAEUS, which is approximately twenty-five minutes long, and, based on the content of the entire recording, seems to have been recorded in late July/early August of 2011. In the recording, [REDACTED] asked PETRAEUS about the location of the "black books." PETRAEUS responded that the

black books are “in a rucksack up there somewhere.” PETRAEUS further stated the black books, “are highly classified, some of them, they don’t have it on it, but I mean there’s code word stuff in there...” Your affiant believes that when PETRAEUS stated that “there’s code word stuff in there,” it is possible that he was indicating that there was special access program information contained in the black books. Moreover, your affiant believes PETRAEUS’s reference to “they don’t have it on it” indicates that the black books do not have the proper classification markings on them. Photographs of the contents of these black books were found during the review of digital and physical evidence recovered during the consensual search of [REDACTED]’s house.

D. Information Regarding PETRAEUS’s Use of Government Laptops

35. During this investigation, FBI Agents interviewed current and former CIA employees about PETRAEUS’s use of a Department of Defense-issued Panasonic Toughbook laptop computer and a CIA-issued Panasonic Toughbook laptop computer. The information below was obtained both through these interviews and from additional information provided by the CIA:

- a. When PETRAEUS was transitioning from DOD to the CIA, there was a meeting during which a DOD Communications Officer requested that a Panasonic Toughbook laptop computer, serial number 0LKSA22428 (hereinafter the “DOD laptop”), used by PETRAEUS be transferred from the property records of the DOD to the CIA. There was no official transfer of property between the DOD and the CIA concerning the laptop; rather, when PETRAEUS left the DOD and became CIA Director, he continued to use the DOD laptop as well as a DOD air

card.⁴ It is believed that PETRAEUS may have been using the DOD laptop for several years prior to his departure from the DOD and before joining the CIA.

- b. CIA employees were aware of PETRAEUS's use of the DOD laptop and were concerned that it posed a security risk. One employee assessed that there was something on the DOD laptop that PETRAEUS did not want the CIA to see. Employees also had security concerns about PETRAEUS's use of the DOD laptop, which, through the aircard, could connect to the Internet, in Temporary Sensitive Compartmented Information Facility environments.
- c. In or around April 2012, PETRAEUS complained to CIA employees that the DOD laptop was running slower than usual. Based on this report, and with PETRAEUS's permission, officials at the CIA conducted a scan of the DOD laptop for viruses. Also, at some point in or around June 2012, PETRAEUS attempted to take the DOD laptop to a private computer vendor because he believed it may have been infected with a virus. Upon learning this, officials at the CIA requested that PETRAEUS not take his computer to a private vendor but rather that he allow employees of the CIA to scan the computer for viruses. Ultimately, PETRAEUS allowed CIA employees to conduct this security scan. Thus, two security scans were conducted on the DOD laptop in April and June 2012. In order to conduct the virus scans, CIA employees created images of the DOD laptop on external hard drives and then ran the virus scans on these images. The scan conducted in April 2012 utilized a Western Digital external hard drive bearing serial number WXN1098Y4486, and the scan conducted in June 2012

⁴ An aircard is a high-speed wireless broadband card that gives users mobile Internet access on their laptops, using cellular data service.

utilized a Western Digital external hard drive bearing serial number WXN208N10851. According to CIA employees, these hard drives contain scanned images of the entire contents of the DOD laptop hard drive as of April 2012 and June 2012.

- d. On or about August 30, 2012, PETRAEUS was provided a CIA-issued Panasonic Toughbook laptop, serial number 1AKYA25016 (hereinafter the "CIA laptop"), and a CIA-issued aircard for use with the CIA laptop. The intended use of the CIA laptop by PETRAEUS was detailed in an internal CIA document which allowed him to use the CIA laptop for non-official business that still had a government nexus. When the CIA laptop was presented to PETRAEUS by CIA staff members, PETRAEUS was informed that the CIA laptop would be scanned for viruses and software updates on a weekly basis. Further, it was reiterated to PETRAEUS that the CIA laptop was a government-issued laptop and that the laptop must be returned to the CIA when he separated from the CIA.
- e. PETRAEUS continued to possess the DOD laptop until on or about October 19, 2012, when he requested that a CIA employee transfer files from his DOD laptop to his CIA laptop. This transfer was accomplished using two separate four-gigabyte USB drives, bearing serial numbers BH1003OCXB and BH1003OBWB. According to CIA employees, these USB drives contain copies of certain files which were transferred from the DOD laptop to the CIA laptop on or about October 19, 2012. After this transfer, a CIA employee maintained possession of the DOD laptop until it was seized and preserved as evidence by members of the CIA Office of Inspector General in November 2012.

- f. Based on an interview of a CIA employee, the CIA laptop provided to PETRAEUS did not have a security banner. This lack of a banner was an uncommon practice at the CIA.
- g. Based on an interview of a CIA employee, PETRAEUS was not known to use computers other than those provided by either the DOD or the CIA. While serving as Director of the CIA, PETRAEUS had access to a CIA computer system that allowed for the processing of unclassified information and also provided access to the Internet. Still, while outside his office or on official travel, PETRAEUS primarily used the DOD laptop to access his military email account. A CIA employee also indicated that PETRAEUS utilized the DOD laptop at home.

36. Based on this description of PETRAEUS's computer use, emails sent to [REDACTED] from PETRAEUS's military email account, as well as emails sent to [REDACTED] using the covert email accounts described above, would likely have been created or viewed from the DOD laptop this affidavit seeks to search.

E. Continuing Communications Between PETRAEUS and [REDACTED]

37. [REDACTED] and PETRAEUS are believed to have had multiple telephonic contacts after each was made aware of FBI Tampa's computer intrusion investigation. Your affiant asserts:

- a. PETRAEUS's CIA Security Detail was notified of the FBI investigation on June 22, 2012. In an interview with FBI Tampa on October 26, 2012, PETRAEUS acknowledged that: (1) he was briefed by the Security Detail concerning the FBI

investigation, and (2) he called [REDACTED] on June 23, 2012 regarding the emails received by Witness 1.

- b. Over the weekend of August 11, 2012 and August 12, 2012, PETRAEUS spoke to Witness 1. In evidence reviewed by FBI Charlotte, a telephone number attributed to [REDACTED] called a telephone number attributed to PETRAEUS on August 11, 2012.
- c. [REDACTED] was interviewed by FBI Tampa on September 24, 25, and 26, 2012. A telephone number attributed to [REDACTED] called a telephone number attributed to PETRAEUS on three occasions on September 25, 2012.
- d. [REDACTED] was in contact with FBI Tampa on October 1 and 2, 2012. These contacts ultimately resulted in a telephone interview conducted on October 3, 2012. In evidence reviewed by FBI Charlotte, on October 2, 2012, there were six calls between telephone numbers attributed to [REDACTED] and PETRAEUS. One of these calls connected, resulting in an approximately fifteen-minute-long conversation.
- e. During the October 26, 2012 interview of PETRAEUS by FBI Tampa, he stated that, while coming back from a trip to the Far East earlier in the month, he called [REDACTED], who told him about her interview with the FBI. Evidence indicated that a telephone number attributed to PETRAEUS called a telephone number attributed to [REDACTED] on October 16, 2012.
- f. Following FBI Tampa's October 26, 2012 interview of PETRAEUS, a telephone number attributed to [REDACTED] called a telephone number attributed to

PETRAEUS on four occasions on October 27, 2012, on three occasions on October 28, 2012, and on two occasions on October 29, 2012.

g. On November 2, 2012, [REDACTED] was again interviewed by FBI Tampa.

[REDACTED] stated that she and PETRAEUS had talked candidly since each of their interviews with the FBI.

h. On November 9, 2012, [REDACTED] contacted FBI Tampa telephonically from telephone number ([REDACTED]) [REDACTED] - [REDACTED]. She advised she received a telephone call from PETRAEUS earlier that day advising her of his resignation. In evidence reviewed by FBI Charlotte, telephone number ([REDACTED]) [REDACTED] - [REDACTED] called a telephone number attributed to PETRAEUS on November 9, 2012.

38. The foregoing telephone communications identified in this affidavit only include calls made or received from one government phone attributed to PETRAEUS. As detailed above, PETRAEUS and [REDACTED] have previously been in regular contact through email, and communicated about the provision of classified information to [REDACTED]. Moreover, [REDACTED] and PETRAEUS have admitted that they established covert communications systems using pre-paid cellular telephones and non-attributable email accounts. To date, the pre-paid telephone numbers used by PETRAEUS and [REDACTED] have not been identified.

39. The DOD laptop as well as the associated external hard drives and the USB drives are currently in the lawful possession of the CIA. As described more fully in paragraph 35 above, the DOD laptop and the associated external hard drives and USB drives came into the CIA's possession in the following way: The DOD laptop was provided by PETRAEUS to a CIA employee on or about October 19, 2012 after relevant files were

transferred to a new CIA-provided laptop. The external hard drives were used to complete virus scans, with PETRAEUS's permission, on the DOD laptop. The USB drives were used to transfer certain files to the CIA laptop. The DOD laptop as well as the associated external hard drives and the USB drives were subsequently seized by the CIA Office of Inspector General for investigative purposes after PETRAEUS's resignation as CIA Director. Therefore, while the CIA might already have all necessary authority to examine the DOD laptop and associated external hard drives and USB drives, I seek this additional warrant out of an abundance of caution to be certain that an examination of the items will comply with the Fourth Amendment and other applicable laws.

40. The DOD laptop as well as the associated external hard drives and the USB drives are currently located in evidence storage in the Office of Inspector General, Central Intelligence Agency, Headquarters Building, Langley, Virginia. It is my understanding that the DOD laptop and associated external hard drives and USB drives have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the items first came into the possession of the CIA Office of Inspector General.

LOCATION TO BE SEARCHED

41. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for the DOD laptop as well as the associated external hard drives and the USB drives, as more fully described in Attachment A to this affidavit, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted

communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

42. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

43. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

44. There is probable cause to believe that things that were once stored on the devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
 - c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
 - d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."
45. Forensic evidence: As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is

evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

46. Nature of examination: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. Searches and seizures of evidence from computers commonly requires agents to download or copy information from the computer and components, and to seize the computer to be processed later by a qualified computer expert in a laboratory or other controlled environment. Searching computer systems for evidence is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover hidden, erased, deleted, compressed, password-protected, or encrypted files. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

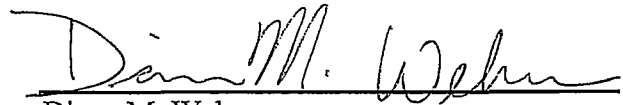
47. Manner of execution: Because this warrant seeks only permission to examine devices already in the government's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

48. Based upon the foregoing, your affiant submits that sufficient probable cause exists for the issuance of a warrant to search the DOD laptop and associated external hard drives and USB drives as further described in Attachments A and B; and that the described laptop contains evidence of a crime relating to: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.


REQUEST FOR SEALING

49. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.



Diane M. Wehner
Special Agent
FBI Charlotte Division

Sworn to and subscribed before me
this 4th day of April, 2013.

 /s/ _____

Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

Property To Be Searched

The property to be searched is as follows:

- One Panasonic Toughbook laptop computer, model number CF-F9KWHZZ1M, serial number 0LKSA22428, hereinafter "the Device."
- Two Western Digital external hard drives, both black in color, bearing serial numbers WXN1098Y4486 and WXN208N10851, hereinafter "the External Hard Drives."
- Two Sandisk Cruzer 4 Gigabyte USB Drives, bearing serial numbers BH1003OCXB and BH1003OBWB, hereinafter "the USB Drives."

The Device, the External Hard Drives, and the USB Drives are currently located in evidence storage in the Office of Inspector General, Central Intelligence Agency, Headquarters Building, Langley, Virginia.

This warrant authorizes the forensic examination of the Device, the External Hard Drives, and the USB Drives for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things To Be Seized

All records or information on the Device, the External Hard Drives, and the USB Drives described in Attachment A that relate to violations of: (a) Title 18, United States Code, Section 1924; (b) Title 18, United States Code, Section 793(e); and (c) Title 18, United States Code, Section 371, including:

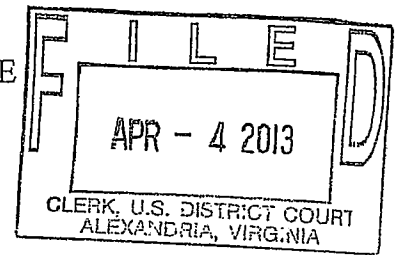
1. All records or information related to any communications between PETRAEUS and [REDACTED];
2. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;
3. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
4. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED];
5. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
6. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

7. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;
8. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS;
9. Any information recording PETRAEUS's schedule or travel from December 2008 to the present;
10. Evidence of user attribution showing who used or owned the Device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, address books, contact lists, saved usernames and passwords, documents, and browsing history; and
11. Records evidencing the use of the Internet, including:
 - i. records of Internet Protocol addresses used;
 - ii. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of social networking and online service usage, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF) UNDER SEAL
ONE PANASONIC LAPTOP COMPUTER,)
TWO WESTERN DIGITAL HARD DRIVES, and) Case No. 1:13sw274
TWO SANDISK CRUZER USB DRIVES)

**GOVERNMENT'S MOTION TO SEAL SEARCH WARRANT
PURSUANT TO LOCAL RULE 49(B)**

Upon the return of its executed search warrant,¹ the United States, by and through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the search warrant, application for the **search warrant** and the **affidavit** in support of the search warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal the search warrant and affidavit.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. At the present time, Special Agents of the Federal Bureau of Investigation are conducting an investigation into, inter alia, the unlawful retention and removal of classified information and the unlawful possession and communication of national defense information, in violation of Title 18, United States Code, Sections 1924 and 793(e).

2. Premature disclosure of the specific details of this ongoing investigation (as reflected, for example, in the affidavit in support of search warrant) would jeopardize this

¹ Pursuant to Local Rule 49(B), "[n]o separate motion to seal is necessary to seal a search warrant *from the time of issuance to the time the executed warrant is returned.*" (Emphasis added.) This is because, as Rule 49(B) additionally mandates, "[u]ntil an executed search warrant is returned, search warrants and related papers are not filed with the Clerk."

continuing criminal investigation, including the ability of the United States to locate and arrest additional persons, and may lead to the destruction of additional evidence in other locations. Thus, a sealing order is necessary to avoid hindering the ongoing investigation in this matter.

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the information there would hamper’ th[e] ongoing investigation.” Media General Operations 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d

514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, regarding the notice requirement in the specific context of a search warrant, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” Media General Operations, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, in the context of search warrants, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. As to the requirement of a court’s consideration of alternatives, the Fourth Circuit counsels that, “[i]f a judicial officer determines that full public access is not appropriate, she ‘must consider alternatives to sealing the documents,’ which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the

subject to the government's motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, “in entering a sealing order, a ‘judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,’” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate “decision to seal the papers “ is “made by the judicial officer,” Goetz, 886 F.2d at 65. “Moreover, if appropriate, the government's submission and the [judicial] officer's reason for sealing the documents can be filed under seal.” Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) (“if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal”).

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

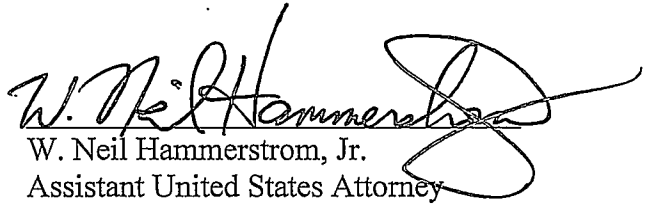
9. Pursuant to Local Rule 49(B)(3), the **search warrant** and the **affidavit** will remain sealed until the need to maintain the confidentiality of the search warrant application and the related investigation expires, after which time the United States will move to unseal the search warrant and affidavit.

WHEREFORE, the United States respectfully requests that the search warrant, application for search warrant, affidavit in support of the search warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court.

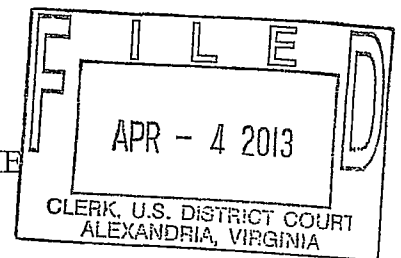
Respectfully submitted,

Neil H. MacBride
United States Attorney

By:


W. Neil Hammerstrom, Jr.
Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA



Alexandria Division

IN THE MATTER OF THE SEARCH OF) UNDER SEAL
ONE PANASONIC LAPTOP COMPUTER,)
TWO WESTERN DIGITAL HARD DRIVES, and) Case No. 1:13sw 274
TWO SANDISK CRUZER USB DRIVES)

ORDER TO SEAL

The UNITED STATES, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, having moved to seal the search warrant, the application for search warrant, the affidavit in support of the search warrant, the Motion to Seal, and proposed Order in this matter; and

The COURT, having considered the government's submissions, including the facts presented by the government to justify sealing; having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED, ADJUDGED, and DECREED that, the search warrant, application for search warrant, affidavit in support of the search warrant, Motion to Seal, and this Order be sealed until further Order of the Court.

Ivan D. Davis /s/
Ivan D. Davis
United States Magistrate Judge

Date: 4 Apr 13
Alexandria, Virginia

COPY

UNITED STATES DISTRICT COURT

for the
Eastern District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)ONE PANASONIC LAPTOP COMPUTER and
ONE VERIZON AIRCARD

Case No. 1:13sw

275

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.**YOU ARE COMMANDED** to execute this warrant on or before April 18, 2013
(not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Ivan D. Davis
(name)☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).
☐ until, the facts justifying, the later specific date of _____.Date and time issued: 9 Apr 13 at 1546 hrs,IDA /s/ _____
Ivan D. Davis
United States Magistrate JudgeCity and state: Alexandria, Virginia

The Honorable Ivan D. Davis

Printed name and title

ATTACHMENT A

Property To Be Searched

The property to be searched is as follows:

- One Panasonic Toughbook laptop computer, model number CF-F9KWHZZ1M, serial number 1AKYA25016, hereinafter "the Device."
- One Verizon Aircard, serial number 105100418696, hereinafter "the Aircard."

The Device and the Aircard are currently located in evidence storage in the Office of Inspector General, Central Intelligence Agency, Headquarters Building, Langley, Virginia.

This warrant authorizes the forensic examination of the Device and the Aircard for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things To Be Seized

All records or information on the Device and the Aircard described in Attachment A that relate to violations of: (a) Title 18, United States Code, Section 1924; (b) Title 18, United States Code, Section 793(e); and (c) Title 18, United States Code, Section 371, including:

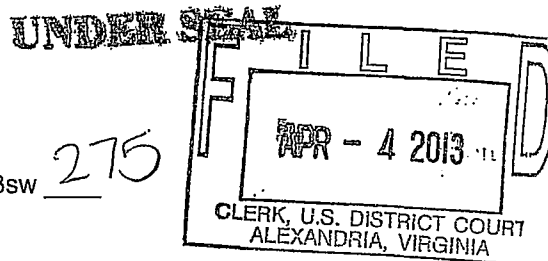
1. All records or information related to any communications between PETRAEUS and [REDACTED];
2. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;
3. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
4. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED];
5. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
6. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

7. All records or information related to any communications, from June 2012 to the present, between PETRAEUS and any other person concerning ongoing law enforcement investigations;
8. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS;
9. Any information recording PETRAEUS's schedule or travel from December 2008 to the present;
10. Evidence of user attribution showing who used or owned the Device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, address books, contact lists, saved usernames and passwords, documents, and browsing history; and
11. Records evidencing the use of the Internet, including:
 - i. records of Internet Protocol addresses used;
 - ii. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of social networking and online service usage, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

ONE PANASONIC LAPTOP COMPUTER and
ONE VERIZON AIRCARD

Case No. 1:13sw

275

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 USC 1924; 18 USC 793(e);
18 USC 371

Unlawful removal and retention of classified documents; unlawful possession and communication of national defense information; conspiracy

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Diane M. Wehner, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

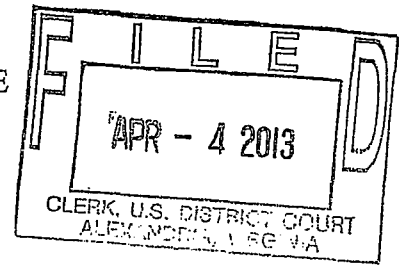
Date: 04/04/2013

City and state: Alexandria, Virginia

/s/
Ivan D. Davis
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF) UNDER SEAL
ONE PANASONIC LAPTOP COMPUTER and)
ONE VERIZON AIRCARD) Case No. 1:13sw 275

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, DIANE M. WEHNER, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search both a government laptop computer used by DAVID PETRAEUS and an aircard used in association with the same government laptop computer.¹ The specifics of the laptop computer and aircard to be searched and items to be seized are more fully described in Attachments A and B, which are incorporated fully by reference herein.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for approximately seven years. I have investigated matters involving complex financial fraud, public corruption, and counterterrorism. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by individuals attempting to conceal their illegal behavior. I have also received specialized training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government

¹ An aircard is a high-speed wireless broadband card that gives users mobile Internet access on their laptops, using cellular data service.

officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.
5. For the reasons set forth below, there is probable cause to believe that the government laptop computer used by PETRAEUS and the associated aircard (both described in detail in Attachment A) contains evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful communication and/or retention of classified information.
6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.
9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."

10. E.O. 13526 also provides that certain senior U.S. officials are authorized to establish “special access programs” upon a finding that “the vulnerability of, or threat to, specific information is exceptional” and “the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.” Within the U.S. Intelligence Community, the Director of National Intelligence is authorized to establish special access programs for intelligence sources, methods, and activities. Such intelligence programs are called “Sensitive Compartmented Information Programs” or SCI Programs.
11. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head’s designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

12. PETRAEUS is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about July 4, 2010 to July 18, 2011, PETRAEUS served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, PETRAEUS served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, PETRAEUS held a United States government security clearance allowing him access to classified United States government information. According to a Department of Defense (DOD) official, to obtain that clearance, PETRAEUS was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled

to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

13. [REDACTED] is a researcher and author of a biography of PETRAEUS, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. According to a DOD official, to obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
14. In 2012, [REDACTED] was the subject of an FBI Tampa Division (FBI Tampa) computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1. This complaint alleged the receipt of threatening and harassing emails from an unknown individual. Witness 1 claimed to have friendships with several high-ranking public and military officials.
15. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of PETRAEUS, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified PETRAEUS's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that PETRAEUS

personally requested that Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that PETRAEUS believed the alleged cyber stalker possessed information which could "embarrass" PETRAEUS and other public officials. Ultimately the FBI determined, based upon the investigation, that [REDACTED] was the individual who had sent the emails to Witness 1.

16. On September 24, 2012 as part of the FBI Tampa investigation, [REDACTED] consented to a search of two laptops and two external hard drives belonging to her. A review of the digital media contained on these devices revealed over 100 items which were identified by FBI Charlotte Computer Analysis Response Team (CART) Forensic Examiners as potentially containing classified information, up to the Secret level.
17. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with [REDACTED]. He denied providing any classified documents to [REDACTED] or having any arrangement to provide her with classified information. PETRAEUS stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.
18. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her

time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from PETRAEUS.

19. During interviews conducted of [REDACTED] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of pre-paid cellular telephones and email accounts using non-attributable names. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if all the accounts were identified because both [REDACTED] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [REDACTED]'s September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

20. On November 12, 2012, Agents from the Charlotte and Tampa Divisions of the FBI participated in a consensual search of [REDACTED]'s residence in Charlotte, North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital

media as well as four boxes and one folder of documents. On this same date, [REDACTED]'s administrative assistant voluntarily provided the FBI with digital media as well as one box of documents which she maintained in her home in relation to her employment with [REDACTED]. A review of the seized materials has identified to date hundreds of potentially classified documents, including more than 300 marked Secret, on digital images maintained on various pieces of electronic media.

21. Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. [REDACTED] traveled into and out of Afghanistan several times between September 2010 and July 2011 to conduct research for a biography on PETRAEUS. During this time, PETRAEUS was serving as the International Security Assistance Force (ISAF) Commander.
22. [REDACTED]'s paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting [REDACTED] access to classified information for the purpose of writing his biography. For example, in an email dated January 16, 2011, which Petraeus marked as CONFIDENTIAL and sent to multiple members of the military, he instructed a member of his staff to "PLS PRINT FOR [REDACTED], ON AN OFF THE RECORD BASIS." Travel documents show that [REDACTED] was in Afghanistan at this time.

A. Communications Regarding Potential Mishandling of Classified Information

23. On May 12, 2011, [REDACTED], using email account [REDACTED], sent an email to PETRAEUS at email account [REDACTED]. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training,

experience, and information reviewed to date in this investigation, your affiant believes the email related to a document or series of documents provided by PETRAEUS to [REDACTED] which contained classified information.

24. Between July 13, 2011 and July 15, 2011, [REDACTED] and a [REDACTED] Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED], emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED] on July 15, 2011, he advised he was working on the storyboards and asked her for "a good SIPR number."² Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) PETRAEUS at email account [REDACTED]. [REDACTED]'s response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel likely reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

25. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED], and PETRAEUS, using email address [REDACTED]

² SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

██████████, discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," ██████████ raised issues which PETRAEUS addressed by typing in all capital letters within the body of ██████████'s original emails. In the email string, while discussing PETRAEUS's files, ██████████ wrote, "[T]he ██████████ letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in ██████████'s email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

26. ██████████ responded: "Thanks for your willingness to get out the boxes! ██████████, the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there."³ In response PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

27. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address ██████████, and ██████████, using email address ██████████, exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "██████████ files" as well as other files and expressed his willingness to share them with ██████████. PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your affiant believes the term "triage" refers to the classified contents of the documents. ██████████ expressed her excitement about PETRAEUS's

³ NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

willingness to share the files writing: “[I]’ll protect them. And I’ll protect you.”

PETRAEUS later responded to [REDACTED], writing, “[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they’re upstairs, but they’re not organized enough at this point...”⁴ PETRAEUS continued, writing, “[A]nd I think MNSTC-I files went to NDU, though I’m not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class’d, but I guess I might share!**” (emphasis added).

28. Your affiant believes that PETRAEUS’s reference to “Class’d” means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified.

B. Audio Recordings Indicating Potential Mishandling of Classified Information

29. PETRAEUS, in his capacity as ISAF Commander, maintained a digital recorder and may have used the recorder to capture select conversations. Your affiant has identified at least five images on the internet which show PETRAEUS with a recorder. One image shows PETRAEUS in military uniform, apparently in Afghanistan, another is a photograph from [REDACTED]’s Facebook account showing PETRAEUS and [REDACTED] sitting together in an office, believed to be PETRAEUS’s office in Afghanistan. Your affiant has reviewed audio files recovered from [REDACTED]’s digital media and identified recorded conversations in which [REDACTED] is not heard on the recording and is not

⁴ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). PETRAEUS was the former commander of MNF-I.

believed to have been present. Based upon the content of these recordings, your affiant believes the recorded conversations were originated by PETRAEUS. Your affiant has reviewed publicly available video and audio voice files of PETRAEUS and believes that the above-referenced recordings do include the voice of PETRAEUS. Investigators have not yet recovered any digital recorders from [REDACTED] or PETRAEUS.

30. In an audio file located on a computer received from [REDACTED]'s administrative assistant, there is a recording of an interview conducted by [REDACTED] during the course of her research on PETRAEUS. This recording is approximately twenty-four minutes, and based on the content of the audio, seems to have been recorded in the August 2011 timeframe. During the recorded conversation, [REDACTED] informed an unknown individual she was interviewing that she would be traveling to Washington, D.C. a lot that month to meet with PETRAEUS and would go through boxes in "his attic."

31. In an audio file located on a hard drive seized from [REDACTED]'s residence on November 12, 2012, there is a recorded conversation between PETRAEUS and, inter alia, Washington Post reporters, which, based on the information and belief of your affiant, occurred in or about March 2011. In the conversation, PETRAEUS stated, "[I] would really love to be on background as a senior military officer." Later in the recording, PETRAEUS discusses sensitive military campaigns and operations, some of which, on the basis of a preliminary review by another government agency designated to assist in this investigation, is believed to contain classified information, including information at the Top Secret level.

32. In an audio file located on electronic evidence seized from [REDACTED]'s residence on November 12, 2012, there is a recorded conversation between PETRAEUS, a reporter, and at least one other individual. During the conversation, PETRAEUS requested that information he provided be attributed to a "defense official familiar with PETRAEUS's activities." PETRAEUS was concerned about the sensitivity of the information he was providing, and wanted to ensure the information was not attributed to him because it would come out after he was confirmed as Director of the CIA. PETRAEUS then discussed with the reporter information that, on the basis of a preliminary review by another government agency designated to assist in this investigation, is believed to be classified, including information at the Top Secret level.

C. Additional Evidence of Potential Mishandling of Classified Information

33. In an email dated June 26, 2011, an Army historian previously assigned to ISAF replied to an email from PETRAEUS in which PETRAEUS discussed [REDACTED]'s research efforts. In the body of the Army historian's response, the historian wrote, "I [am] happy to receive [REDACTED]'s research effort and will add it to the collection. It is still my understanding that your 'black books' and other sensitive items are off limits. She can look at the other documents such as update briefs, info papers, photos, and other reference materials, but not the sensitive ones. Am I correct on that rule?"

34. In an audio file located on a laptop computer seized from [REDACTED], there is a recorded conversation between [REDACTED] and PETRAEUS, which is approximately twenty-five minutes long, and, based on the content of the entire recording, seems to have been recorded in late July/early August of 2011. In the recording, [REDACTED] asked PETRAEUS about the location of the "black books." PETRAEUS responded that the

black books are “in a rucksack up there somewhere.” PETRAEUS further stated the black books, “are highly classified, some of them, they don’t have it on it, but I mean there’s code word stuff in there...” Your affiant believes that when PETRAEUS stated that “there’s code word stuff in there,” it is possible that he was indicating that there was special access program information contained in the black books. Moreover, your affiant believes PETRAEUS’s reference to “they don’t have it on it” indicates that the black books do not have the proper classification markings on them. Photographs of the contents of these black books were found during the review of digital and physical evidence recovered during the consensual search of [REDACTED]’s house.

D. Information Regarding PETRAEUS’s Use of Government Laptops

35. During this investigation, FBI Agents interviewed current and former CIA employees about PETRAEUS’s use of a Department of Defense-issued Panasonic Toughbook laptop computer and a CIA-issued Panasonic Toughbook laptop computer. The information below was obtained both through these interviews and from additional information provided by the CIA:

- a. When PETRAEUS was transitioning from DOD to the CIA, there was a meeting during which a DOD Communications Officer requested that a Panasonic Toughbook laptop computer, serial number 0LKSA22428 (hereinafter the “DOD laptop”), used by PETRAEUS be transferred from the property records of the DOD to the CIA. There was no official transfer of property between the DOD and the CIA concerning the laptop; rather, when PETRAEUS left the DOD and became CIA Director, he continued to use the DOD laptop as well as a DOD air

card. It is believed that PETRAEUS may have been using the DOD laptop for several years prior to his departure from the DOD and before joining the CIA.

- b. CIA employees were aware of PETRAEUS's use of the DOD laptop and were concerned that it posed a security risk. One employee assessed that there was something on the DOD laptop that PETRAEUS did not want the CIA to see. Employees also had security concerns about PETRAEUS's use of the DOD laptop, which, through the aircard, could connect to the Internet, in Temporary Sensitive Compartmented Information Facility environments.
- c. In or around April 2012, PETRAEUS complained to CIA employees that the DOD laptop was running slower than usual. Based on this report, and with PETRAEUS's permission, officials at the CIA conducted a scan of the DOD laptop for viruses. Also, at some point in or around June 2012, PETRAEUS attempted to take the DOD laptop to a private computer vendor because he believed it may have been infected with a virus. Upon learning this, officials at the CIA requested that PETRAEUS not take his computer to a private vendor but rather that he allow employees of the CIA to scan the computer for viruses. Ultimately, PETRAEUS allowed CIA employees to conduct this security scan. Thus, two security scans were conducted on the DOD laptop in April and June 2012. In order to conduct the virus scans, CIA employees created images of the DOD laptop on external hard drives and then ran the virus scans on these images. The scan conducted in April 2012 utilized a Western Digital external hard drive bearing serial number WXN1098Y4486, and the scan conducted in June 2012 utilized a Western Digital external hard drive bearing serial number

WXN208N10851. According to CIA employees, these hard drives contain scanned images of the entire contents of the DOD laptop hard drive as of April 2012 and June 2012.

- d. On or about August 30, 2012, PETRAEUS was provided a CIA-issued Panasonic Toughbook laptop, serial number 1AKYA25016 (hereinafter the "CIA laptop"), and a CIA-issued aircard for use with the CIA laptop. The intended use of the CIA laptop by PETRAEUS was detailed in an internal CIA document which allowed him to use the CIA laptop for non-official business that still had a government nexus. When the CIA laptop was presented to PETRAEUS by CIA staff members, PETRAEUS was informed that the CIA laptop would be scanned for viruses and software updates on a weekly basis. Further, it was reiterated to PETRAEUS that the CIA laptop was a government-issued laptop and that the laptop must be returned to the CIA when he separated from the CIA.
- e. PETRAEUS continued to possess the DOD laptop until on or about October 19, 2012, when he requested that a CIA employee transfer files from his DOD laptop to his CIA laptop. This transfer was accomplished using two separate four-gigabyte USB drives, bearing serial numbers BH1003OCXB and BH1003OBWB. According to CIA employees, these USB drives contain copies of certain files which were transferred from the DOD laptop to the CIA laptop on or about October 19, 2012. After this transfer, a CIA employee maintained possession of the DOD laptop until it was seized and preserved as evidence by members of the CIA Office of Inspector General in November 2012.

- f. Based on an interview of a CIA employee, the CIA laptop provided to PETRAEUS did not have a security banner. This lack of a banner was an uncommon practice at the CIA.
- g. Based on an interview of a CIA employee, PETRAEUS was not known to use computers other than those provided by either the DOD or the CIA. While serving as Director of the CIA, PETRAEUS had access to a CIA computer system that allowed for the processing of unclassified information and also provided access to the Internet. Still, while outside his office or on official travel, PETRAEUS primarily used the DOD laptop to access his military email account. A CIA employee also indicated that PETRAEUS utilized the DOD laptop at home.

36. Based on this description of PETRAEUS's computer use, emails sent to [REDACTED] from PETRAEUS's military email account, as well as emails sent to [REDACTED] using the covert email accounts described above, would likely have been created or viewed from the CIA laptop this affidavit seeks to search.

E. Continuing Communications Between PETRAEUS and [REDACTED]

37. [REDACTED] and PETRAEUS are believed to have had multiple telephonic contacts after each was made aware of FBI Tampa's computer intrusion investigation. Your affiant asserts:

- a. PETRAEUS's CIA Security Detail was notified of the FBI investigation on June 22, 2012. In an interview with FBI Tampa on October 26, 2012, PETRAEUS acknowledged that: (1) he was briefed by the Security Detail concerning the FBI

investigation, and (2) he called [REDACTED] on June 23, 2012 regarding the emails received by Witness 1.

- b. Over the weekend of August 11, 2012 and August 12, 2012, PETRAEUS spoke to Witness 1. In evidence reviewed by FBI Charlotte, a telephone number attributed to [REDACTED] called a telephone number attributed to PETRAEUS on August 11, 2012.
- c. [REDACTED] was interviewed by FBI Tampa on September 24, 25, and 26, 2012. A telephone number attributed to [REDACTED] called a telephone number attributed to PETRAEUS on three occasions on September 25, 2012.
- d. [REDACTED] was in contact with FBI Tampa on October 1 and 2, 2012. These contacts ultimately resulted in a telephone interview conducted on October 3, 2012. In evidence reviewed by FBI Charlotte, on October 2, 2012, there were six calls between telephone numbers attributed to [REDACTED] and PETRAEUS. One of these calls connected, resulting in an approximately fifteen-minute-long conversation.
- e. During the October 26, 2012 interview of PETRAEUS by FBI Tampa, he stated that, while coming back from a trip to the Far East earlier in the month, he called [REDACTED], who told him about her interview with the FBI. Evidence indicated that a telephone number attributed to PETRAEUS called a telephone number attributed to [REDACTED] on October 16, 2012.
- f. Following FBI Tampa's October 26, 2012 interview of PETRAEUS, a telephone number attributed to [REDACTED] called a telephone number attributed to

PETRAEUS on four occasions on October 27, 2012, on three occasions on October 28, 2012, and on two occasions on October 29, 2012.

g. On November 2, 2012, [REDACTED] was again interviewed by FBI Tampa.

[REDACTED] stated that she and PETRAEUS had talked candidly since each of their interviews with the FBI.

h. On November 9, 2012, [REDACTED], contacted FBI Tampa telephonically from telephone number ([REDACTED]) [REDACTED]-[REDACTED]. She advised she received a telephone call from PETRAEUS earlier that day advising her of his resignation. In evidence reviewed by FBI Charlotte, telephone number ([REDACTED]) [REDACTED]-[REDACTED] called a telephone number attributed to PETRAEUS on November 9, 2012.

38. The foregoing telephone communications identified in this affidavit only include calls made or received from one government phone attributed to PETRAEUS. As detailed above, PETRAEUS and [REDACTED] have previously been in regular contact through email, and communicated about the provision of classified information to [REDACTED]. Moreover, [REDACTED] and PETRAEUS have admitted that they established covert communications systems using pre-paid cellular telephones and non-attributable email accounts. To date, the pre-paid telephone numbers used by PETRAEUS and [REDACTED] have not been identified.

39. The CIA laptop and the associated air card are currently in the lawful possession of the CIA. As described more fully in paragraph 35 above, the CIA laptop and air card came into the CIA's possession in the following way: The CIA laptop was provided to PETRAEUS by CIA personnel on or about August 30, 2012. On or about October 19, 2012, certain files were transferred to the CIA laptop. The CIA laptop and air card were

subsequently seized by the CIA Office of Inspector General for investigative purposes after PETRAEUS's resignation as CIA Director. Therefore, while the CIA might already have all necessary authority to examine the CIA laptop and air card, I seek this additional warrant out of an abundance of caution to be certain that an examination of the items will comply with the Fourth Amendment and other applicable laws.

40. The CIA laptop and air card are currently located in evidence storage in the Office of Inspector General, Central Intelligence Agency, Headquarters Building, Langley, Virginia. It is my understanding that the CIA laptop and air card have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the items first came into the possession of the CIA Office of Inspector General.

LOCATION TO BE SEARCHED

41. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for the CIA laptop computer and associated aircard, as more fully described in Attachment A to this affidavit to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

42. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
43. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.
44. There is probable cause to believe that things that were once stored on the devices may still be stored there, for at least the following reasons:
- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
 - b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

45. Forensic evidence: As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage

medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

46. Nature of examination: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. Searches and seizures of evidence from computers commonly requires agents to download or copy information from the computer and components, and to seize the computer to be processed later by a qualified computer expert in a laboratory or other controlled environment. Searching computer systems for evidence is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover hidden, erased, deleted, compressed, password-protected, or encrypted files. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

47. Manner of execution: Because this warrant seeks only permission to examine devices already in the government's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

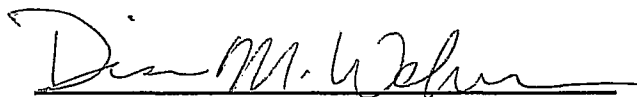
CONCLUSION

48. Based upon the foregoing, your affiant submits that sufficient probable cause exists for the issuance of a warrant to search the CIA laptop and associated aircard as further described in Attachments A and B; and that the described laptop contains evidence of a

crime relating to: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

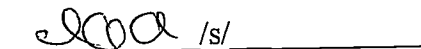
REQUEST FOR SEALING

49. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.



Diane M. Wehner
Special Agent
FBI Charlotte Division

Sworn to and subscribed before me
this 4th day of April, 2013.


Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

Property To Be Searched

The property to be searched is as follows:

- One Panasonic Toughbook laptop computer, model number CF-F9KWHZZ1M, serial number 1AKYA25016, hereinafter "the Device."
- One Verizon Aircard, serial number 105100418696, hereinafter "the Aircard."

The Device and the Aircard are currently located in evidence storage in the Office of Inspector General, Central Intelligence Agency, Headquarters Building, Langley, Virginia.

This warrant authorizes the forensic examination of the Device and the Aircard for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things To Be Seized

All records or information on the Device and the Aircard described in Attachment A that relate to violations of: (a) Title 18, United States Code, Section 1924; (b) Title 18, United States Code, Section 793(e); and (c) Title 18, United States Code, Section 371, including:

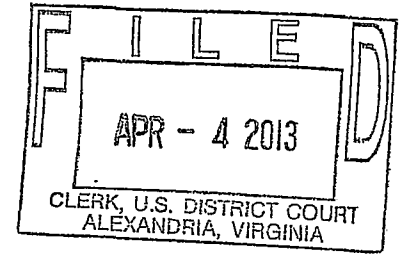
1. All records or information related to any communications between PETRAEUS and [REDACTED];
2. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;
3. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
4. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED];
5. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
6. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

7. All records or information related to any communications, from June 2012 to the present, between PETRAEUS and any other person concerning ongoing law enforcement investigations;
8. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS;
9. Any information recording PETRAEUS's schedule or travel from December 2008 to the present;
10. Evidence of user attribution showing who used or owned the Device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, address books, contact lists, saved usernames and passwords, documents, and browsing history; and
11. Records evidencing the use of the Internet, including:
 - i. records of Internet Protocol addresses used;
 - ii. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of social networking and online service usage, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF) UNDER SEAL
ONE PANASONIC LAPTOP COMPUTER and)
ONE VERIZON AIRCARD) Case No. 1:13sw 275

**GOVERNMENT'S MOTION TO SEAL SEARCH WARRANT
PURSUANT TO LOCAL RULE 49(B)**

Upon the return of its executed search warrant,¹ the United States, by and through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the search warrant, application for the **search warrant** and the **affidavit** in support of the search warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal the search warrant and affidavit.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. At the present time, Special Agents of the Federal Bureau of Investigation are conducting an investigation into, inter alia, the unlawful retention and removal of classified information and the unlawful possession and communication of national defense information, in violation of Title 18, United States Code, Sections 1924 and 793(e).

2. Premature disclosure of the specific details of this ongoing investigation (as reflected, for example, in the affidavit in support of search warrant) would jeopardize this

¹ Pursuant to Local Rule 49(B), "[n]o separate motion to seal is necessary to seal a search warrant *from the time of issuance to the time the executed warrant is returned.*" (Emphasis added.) This is because, as Rule 49(B) additionally mandates, "[u]ntil an executed search warrant is returned, search warrants and related papers are not filed with the Clerk."

continuing criminal investigation, including the ability of the United States to locate and arrest additional persons, and may lead to the destruction of additional evidence in other locations.

Thus, a sealing order is necessary to avoid hindering the ongoing investigation in this matter.

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the information there would hamper’ th[e] ongoing investigation.” Media General Operations 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d

514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and © provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, regarding the notice requirement in the specific context of a search warrant, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” Media General Operations, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, in the context of search warrants, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. As to the requirement of a court’s consideration of alternatives, the Fourth Circuit counsels that, “[i]f a judicial officer determines that full public access is not appropriate, she ‘must consider alternatives to sealing the documents,’ which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the

subject to the government's motion to seal." Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, "in entering a sealing order, a 'judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,'" Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate "decision to seal the papers " is "made by the judicial officer," Goetz, 886 F.2d at 65. "Moreover, if appropriate, the government's submission and the [judicial] officer's reason for sealing the documents can be filed under seal." Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) ("if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal").

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

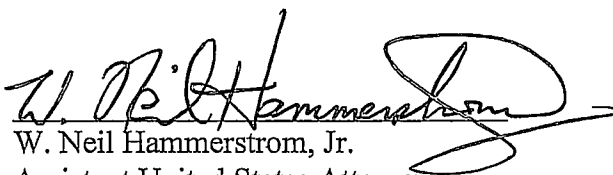
9. Pursuant to Local Rule 49(B)(3), the **search warrant** and the **affidavit** will remain sealed until the need to maintain the confidentiality of the search warrant application and the related investigation expires, after which time the United States will move to unseal the search warrant and affidavit.

WHEREFORE, the United States respectfully requests that the search warrant, application for search warrant, affidavit in support of the search warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court.

Respectfully submitted,

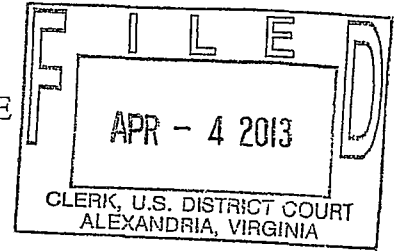
Neil H. MacBride
United States Attorney

By:


W. Neil Hammerstrom, Jr.
Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF) UNDER SEAL
ONE PANASONIC LAPTOP COMPUTER and)
ONE VERIZON AIRCARD)


Case No. 1:13sw 275

ORDER TO SEAL

The UNITED STATES, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, having moved to seal the search warrant, the application for search warrant, the affidavit in support of the search warrant, the Motion to Seal, and proposed Order in this matter; and

The COURT, having considered the government's submissions, including the facts presented by the government to justify sealing; having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED, ADJUDGED, and DECREED that, the search warrant, application for search warrant, affidavit in support of the search warrant, Motion to Seal, and this Order be sealed until further Order of the Court.

 /s/_____
Ivan D. Davis
United States Magistrate Judge

Date: 4 Apr 13
Alexandria, Virginia

UNITED STATES DISTRICT COURT

for the
Western District of North CarolinaFILED
CHARLOTTE, NC

APR 4 2013

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)The Premises Located at [REDACTED]
[REDACTED] as described in Affidavit
and Attachments, incorporated herein.Case No. 3:13-mj-99
US District Court
Western District of NC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A, which is incorporated fully herein.located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):
See Attachment B, which is incorporated fully herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 1924; 18 USC 793(e);	Unauthorized removal and retention of classified documents or material;
18 USC 371	Unauthorized possession, communication, and willful retention of national defense information; Conspiracy

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Certified to be a true and
correct copy of the original.U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.By: B. Tehting
Deputy ClerkDate 4/4/13141-13011-1

Applicant's signature

Gerd J. Ballner, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 04/03/2013Robert J. Conrad

Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr., United States District Court Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Gerd J. Ballner, Jr., being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search the residence of [REDACTED], residing at [REDACTED]. The premises to be searched and items to be seized are more fully described in Attachments A and B.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for approximately thirteen years. I have investigated matters involving National Security to include Counterintelligence and Espionage. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by hostile foreign intelligence services and their recruited human sources to illegally obtain, through clandestine action, classified and proprietary information, which if compromised poses risk to the national security of the United States. I have also received specialized training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

LOCATION TO BE SEARCHED

4. As set forth below, your affiant submits that probable cause exists for the issuance of a search warrant for [REDACTED] residence, as more fully described in Attachment A to this affidavit, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.
5. On March 29, 2013, your affiant conducted a search of the CLEAR public source database for [REDACTED] and determined that her current address of record is [REDACTED]
[REDACTED]. According to 2011 tax records filed in Mecklenburg County, North Carolina, this home is owned by [REDACTED] and [REDACTED]
[REDACTED], and it is further described as a [REDACTED]
[REDACTED]. The house number [REDACTED] is visible as brass numerals on the molding above the front entry door.

STATUTORY AUTHORITY

6. The FBI has been conducting an investigation of [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code,

Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.

7. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

8. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

9. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.

10. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original

classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."

11. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

12. David Petraeus is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, Petraeus served as Commander of the United States Central Command. From on or about July 4, 2010 to July 18, 2011, Petraeus served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, Petraeus served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, Petraeus held a United States government security clearance allowing him access to classified United States government information. According to a Department of Defense (DOD) official, to obtain that clearance, Petraeus was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to

receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

13. [REDACTED] is a researcher and author of a biography of Petraeus, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. According to a DOD official, to obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
14. In June 2012, the FBI's Tampa Division (FBI Tampa) opened a computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1, which alleged the receipt of threatening and harassing emails from the email addresses [REDACTED] and [REDACTED]. Witness 1 claimed friendships with several high-ranking public and military officials.
15. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of Petraeus, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified Petraeus's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that Petraeus personally requested that

Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that Petraeus believed the alleged cyber stalker possessed information which could "embarrass" Petraeus and other public officials.

16. Investigation conducted by FBI Tampa identified [REDACTED] as the person suspected of using the email accounts [REDACTED] and [REDACTED]. Investigation also determined [REDACTED] uses the email account [REDACTED]. On September 24, 2012, FBI Tampa interviewed [REDACTED] at her residence. During this interview [REDACTED] admitted sending the emails to Witness 1, as well as other emails regarding Witness 1 to senior United States military officers as well as a foreign diplomat. [REDACTED] also stated that she had engaged in an extramarital affair with Petraeus. [REDACTED] provided consent to search two of her laptop computers and two external hard drives.

17. On September 25, 2012, FBI Tampa returned [REDACTED] laptop computers and conducted a follow-up interview. During this follow-up interview, [REDACTED] admitted she told Petraeus that he should get Witness 1 to "drop the charges." [REDACTED] advised she does not know if Petraeus made the request of Witness 1. During the course of this interview, [REDACTED] provided interviewing agents consent to search her Apple iPhone, which she had in her possession. FBI Charlotte Computer Analysis Response Team (CART) Forensic Examiners copied the contents of her Apple iPhone at the interview location. This iPhone, serial number C28J60GKDTDD, is believed to be the same iPhone currently in [REDACTED] possession. It was returned

to [REDACTED] at the conclusion of the interview.¹ A review of [REDACTED] laptops and external hard drives located over 100 items which were identified by Charlotte CART Forensic Examiners as containing potentially classified information, including information up to the Secret level.

18. On October 26, 2012, Petraeus was interviewed at CIA Headquarters. Petraeus stated that he had had an extramarital affair with [REDACTED]. He denied providing any classified documents to [REDACTED] or having any arrangement to provide her with classified information. Petraeus stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.

19. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about Petraeus; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes

¹ Because the consensual search of the iPhone was conducted as part of FBI Tampa's computer intrusion investigation, FBI Charlotte has not reviewed the forensic images of the iPhone.

obtain a paper copy of the briefings to preserve the information as research for her book.

██████████ advised that she never received classified information from Petraeus.

20. During interviews conducted of ██████████ and Petraeus under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with one another. These methods included the use of pre-paid cellular telephones and email accounts using non-attributable names. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if all the accounts were identified because both ██████████ and Petraeus stated they could not recall all the account names which they created and used to communicate. During ██████████ September 25, 2012 interview, she advised that she and Petraeus would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

A. ██████████ Consensual Search, November 12, 2012

21. As a result of finding potentially classified information on the laptops provided by ██████████, FBI Tampa and FBI Charlotte conducted a consensual search of ██████████ Charlotte residence on November 12, 2012 to recover any evidence related to cyber stalking, in violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents or material, in violation of 18 U.S.C. § 1924. On this same date, a consensual search was also conducted at the residence of ██████████ administrative assistant, ██████████, in Concord, North Carolina. ██████████ voluntarily provided the FBI with various items she maintained in her home in relation to her employment with ██████████. During the searches, additional paper documents were found, some of which, upon belief and information of

your affiant, are classified. As a result of the two searches, the following digital media were seized: eight computers, twelve external hard drives, two printers/scanners, two cellular telephones, two Apple iPods, seven thumbdrives/memory cards, and approximately fifty floppy discs, CDs, and optical discs.

22. Based on a preliminary review of [REDACTED] digital media, it is believed she came into possession of potentially classified information both before and during the writing of her book, "All In: The Education of General David Petraeus." Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. Given her extensive use of digital media, your affiant believes [REDACTED] received/exchanged classified information via email and/or made contact with individuals via email and/or telephone to schedule in-person meetings for the purpose of recording and collecting classified information, as detailed below. [REDACTED] is also believed to have digitally stored numerous documents, photographs, and audio interviews which contain classified information.

B. Additional Evidence of Potential Mishandling of Classified Information

23. A review of [REDACTED] digital media has identified photographs of at least two black books, which appear to be the daily event and calendar books used by Petraeus to memorialize significant events during his military assignments.² Investigators have reviewed the metadata from some of the digital media obtained consensually from [REDACTED] and have determined that from on or about August 29, 2011 to on or about August 31, 2011, there were approximately one hundred and seventeen separate

² Based on a review of these photographs and their embedded metadata, your affiant believes that all of the photographs referenced in paragraphs 23 through 28 of this affidavit were taken using [REDACTED] iPhone.

photographs taken of the contents of the black books. These photographs have been reviewed by your affiant in close coordination with other government agencies designated to assist with this investigation. Based upon a preliminary review by another government agency designated to assist in this investigation, your affiant has reason to believe that at least five of these photographs contain classified information, including information up to the Top Secret level.

24. Additional review of embedded metadata, including date and time stamps, allowed investigators to identify specific photographs from [REDACTED] digital media. On August 29, 2011, at 9:47 a.m., two photographs were taken of the front cover of a black book which had Petraeus's personal business card taped to the front cover. The business card identified Petraeus as "General David H. Petraeus, Commander, International Security Assistance Force."
25. Open source information includes a photograph depicting Petraeus with a black book. See www.thedailybeast.com/newsweek/2011/07/17/general-david-petraeus-on-leaving-afghanistan-and-going-to-cia.html. Based on my review, I believe that the black book depicted in the photographs described in paragraph 24 above is the same black book depicted in the photograph of Petraeus in the news article on the above-mentioned website. The photograph shows Petraeus, while in Afghanistan, standing with then-Secretary of Defense Leon Panetta and General John Allen. This photograph, dated July 9, 2011, reportedly captured Petraeus while he was ending his command in Afghanistan. On the table next to Petraeus in the same photograph, is a similarly sized black book with a business card taped to the front. The format of the business card, its position on the book, the manner in which it is taped to the book, and its general characteristics are very

similar to the photographs of the front cover of a black book located on [REDACTED]

digital media.

26. Photographs of what appear to be this same black book were taken on August 30, 2011 at 11:21 a.m., 11:22 a.m., 11:28 a.m., 12:09 p.m., and on August 31, 2011 at 6:15 a.m.

Based upon a preliminary review by another government agency designated to assist with this investigation, your affiant has reason to believe these photographs depict pages from the black books containing classified information, including classified information at up to the Top Secret level.

27. An 8.5 x 11 inch sized printed photograph was located during the consensual search of [REDACTED] residence on November 12, 2012. This photograph showed the content of a black book, specifically a page containing a daily calendar for December 3, 2010 on the left side of the notebook and handwritten notes on the right side of the notebook. The written entry on the top line read, "[REDACTED]: C-N Community of Interest." The calendar in the photograph reflected a "CN Briefing" between 1:45 p.m. and 2:30 p.m. on December 3, 2010. Your affiant opines that the written note for [REDACTED] was added by Petraeus so as to provide [REDACTED] context in reading that day's calendar entry. An initial review of the calendar and notes on this specific image revealed a reference to military units and potential needs for these units.

28. Additional review of [REDACTED] digital media also revealed multiple photographs taken between August 16, 2011 and August 17, 2011. On review of the photographs and the embedded metadata, investigators have determined the following:

- a. On August 16, 2011 at 11:04 p.m., a photograph was taken of at least three medium-sized cardboard boxes sitting on a bed. In the photograph, the boxes are

open, and although the contents are unknown, there appear to be some file folders visible inside the boxes. Sitting on the bed next to the boxes is a black laptop computer which is open and powered on, though the screen image is difficult to discern.

- b. On August 16, 2011 at 11:04 p.m., a second photograph from a different angle was taken of the same boxes referenced above. The boxes are open, and one box has the letters "Petrae" written in black and clearly visible on the side. Your affiant believes this writing spelled out "Petraeus," as the "us" in "Petraeus" was partially obscured.
- c. On August 17, 2011 at 9:23 a.m., [REDACTED] is observed in a photograph which she took of herself in a mirror. In the photograph, [REDACTED] is posing next to the same bed mentioned in paragraphs 33a and 33b above. In this photograph, what appear to be two of the same boxes are visible on the bed. The boxes are open, though the contents of the boxes cannot be clearly discerned.

C. Continuing Communications Between [REDACTED] and Petraeus

29. [REDACTED] and Petraeus are believed to have had multiple telephonic contacts after each was made aware of FBI Tampa's computer intrusion investigation. Your affiant asserts:

- a. Petraeus's CIA security detail was notified of the FBI investigation on June 22, 2012. In an interview with FBI Tampa on October 26, 2012, Petraeus acknowledged that: (1) he was briefed by the security detail concerning the FBI investigation, and (2) he called [REDACTED] on June 23, 2012 regarding the emails received by Witness 1.

- b. Over the weekend of August 11, 2012 and August 12, 2012, Petraeus spoke to Witness 1. In evidence reviewed by FBI Charlotte, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on August 11, 2012.³
- c. [REDACTED] was interviewed by FBI Tampa on September 24, 25, and 26, 2012. A telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on three occasions on September 25, 2012.
- d. [REDACTED] was in contact with FBI Tampa on October 1 and 2, 2012. These contacts ultimately resulted in a telephone interview conducted on October 3, 2012. In evidence reviewed by FBI Charlotte, on October 2, 2012, there were six calls between telephone numbers attributed to [REDACTED] and Petraeus. One of these calls connected, resulting in an approximately fifteen-minute-long conversation.
- e. During the October 26, 2012 interview of Petraeus by FBI Tampa, he stated that, while coming back from a trip to the Far East earlier in the month, he called [REDACTED], who told him about her interview with the FBI. Evidence indicated that a telephone number attributed to Petraeus called a telephone number attributed to [REDACTED] on October 16, 2012.
- f. Following FBI Tampa's interview of Petraeus on October 26, 2012, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on four occasions on October 27, 2012, on three occasions on October 28, 2012, and on two occasions on October 29, 2012.

³ Unless otherwise noted, the "telephone number associated with [REDACTED]" in these subparagraphs was [REDACTED], the mobile telephone number used on her current iPhone.

g. On November 2, 2012, [REDACTED] was again interviewed by FBI Tampa.

[REDACTED] stated that she and Petraeus had talked candidly since each of their interviews with the FBI.

h. On November 9, 2012, [REDACTED], contacted FBI Tampa telephonically from telephone number [REDACTED]. She advised she received a telephone call from Petraeus earlier that day advising her of his resignation. In evidence reviewed by FBI Charlotte, telephone number [REDACTED] called a telephone number attributed to Petraeus on November 9, 2012.

30. The foregoing telephone communications identified in this affidavit only include calls made or received from one government phone attributed to Petraeus. As detailed above, Petraeus and [REDACTED] have previously been in regular contact through email, and communicated about the provision of classified information to [REDACTED]. Moreover, [REDACTED], and Petraeus have admitted that they established covert communications systems using pre-paid cellular telephones and non-attributable email accounts. To date, the pre-paid telephone numbers used by Petraeus and [REDACTED] have not been identified.

31. These telephonic contacts and attempted telephonic contacts between telephone numbers attributed to [REDACTED] and Petraeus indicate [REDACTED] relationship with Petraeus continued after their interviews with FBI Tampa in September and October 2012.

32. Considering these facts, and given [REDACTED] history of email and telephone communication with Petraeus, as well as the numerous photographs of what, based on a preliminary review, appear to be classified materials, there is probable cause to believe

that [REDACTED] iPhone contains classified information as well as substantive communications regarding the content of [REDACTED] and Petraeus's FBI interviews, including additional information regarding [REDACTED] access to and retention of classified information.

33. During the consensual search of [REDACTED] Charlotte residence on November 12, 2012, investigators recovered a damaged Apple iPhone, serial number 61116264A4S. Many of the photographs of the black books and cardboard boxes referenced above were located on this damaged iPhone. A review of voicemail and call logs indicates that the damaged iPhone was last used by [REDACTED] in April 2012.
34. Based on your affiant's experience, Apple iPhones allow for the transfer of a user's contents from one telephone to another. It is plausible that [REDACTED], when she ceased using the damaged iPhone, would have transferred data from her damaged iPhone to her current iPhone. Since the damaged iPhone contained photographs of what, based on a preliminary review, appear to be classified materials, and with the potential for transfer of data to her current iPhone, there is probable cause to believe that these photographs were transferred to the iPhone currently in [REDACTED] possession.

TECHNICAL TERMS RELATED TO THE SEARCH

35. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or

traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other

digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive email. PDAs

usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

36. As described above and in Attachment B, this application seeks permission to search for records that might be found on the premises, in whatever form they are found. One form in which the records might be found is data stored on an electronic device. In particular, this application seeks permission to seize an Apple iPhone (hereinafter "the Device"), which could transmit and store such data. Thus, the warrant applied for would authorize the seizure of the Apple iPhone under Rule 41(e)(2)(B).
37. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time, including text messages. Texts messages sent or received on a cellular phone can be stored on a cellular phone at little or no cost. Even when text messages have been deleted by the user of a cellular phone, those text messages, or remnants of those deleted text files, can be recovered months after they have been deleted from a cellular phone. This is so because when a user of a cellular phone "deletes" a text message, the data contained in that message does not actually disappear; rather, that data remains on the cellular phone until it is overwritten with new data. Deleted text messages, or remnants of deleted text messages, may reside on the cellular phone for long periods of time before they are overwritten. Such data can sometimes be recovered with forensic tools.
38. Forensic evidence: As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when.

There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to unlawfully communicate and/or retain classified information, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

39. Necessity of seizing or copying entire computers or storage media: In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with

the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises.

However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

40. Nature of examination: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. Searches and seizures of evidence from computers commonly requires agents to download or copy information from the computer and components, and to seize the computer to be processed later by a qualified computer expert in a laboratory or other controlled environment. Searching computer systems for evidence is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover hidden, erased, deleted, compressed, password-protected, or encrypted files. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

41. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, emails, texts, email addresses used, IP address information, and internet browsing history.

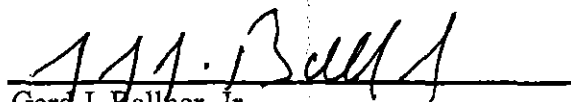
CONCLUSION

42. Based upon the foregoing, your affiant submits that sufficient probable cause exists for the issuance of a warrant to search [REDACTED] [REDACTED], as further described in Attachments A and B; and that the described premises contains evidence of a crime relating to: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

REQUEST FOR SEALING


43. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Respectfully submitted,


Gerald J. Ballher, Jr.
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me

on this, the 3d day of April, 2013.


ROBERT J. CONRAD, JR.
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A

Property To Be Searched

This warrant applies to a single family home and adjoining two-car garage owned by

[REDACTED]

, located at

[REDACTED]

[REDACTED]

. This property is further described as

[REDACTED]

[REDACTED]

which sits on the corner of

[REDACTED]

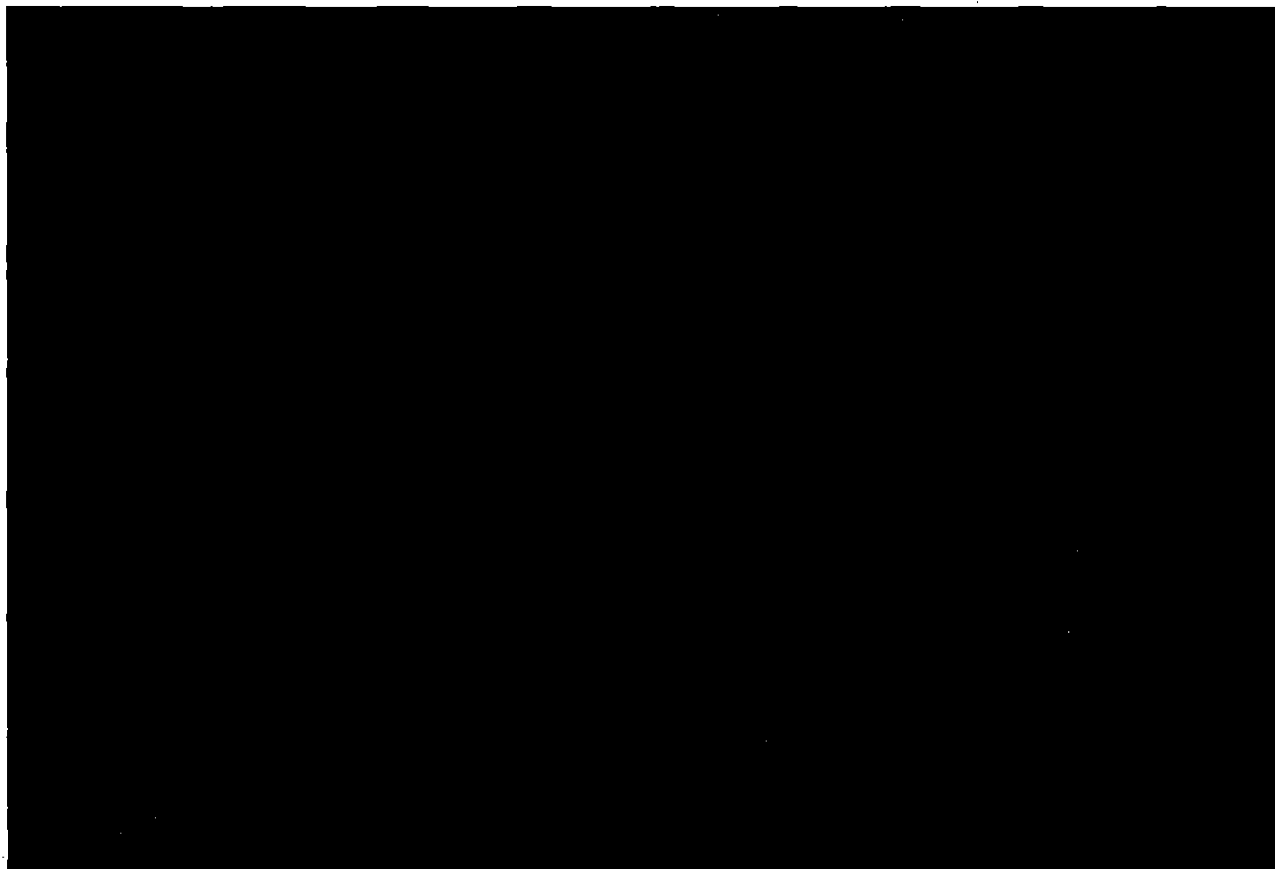
[REDACTED]

The house number

[REDACTED]

is visible as brass numerals on the molding above

the front entry door. A photograph of the residence is provided below:



ATTACHMENT B

Particular Thing To Be Seized

Apple iPhone, serial number C28J60GKDTDD, hereinafter "the Device."

Information To Be Seized by the Government

1. All records or information on the Device that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant, including:
 - a. All records or information related to any communications between [REDACTED] and Petraeus;
 - b. All records or information related to any communications, from December 2008 to the present, between [REDACTED] and any other person or entity concerning classified and/or national defense information;
 - c. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
 - d. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED];
 - e. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
 - f. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

- g. All records or information related to any communications from June 2012 to the present between [REDACTED] and any other person concerning ongoing law enforcement investigations;
 - h. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by [REDACTED] or Petraeus;
 - i. Any information recording [REDACTED] or Petraeus's schedule or travel from December 2008 to the present;
 - j. Evidence of user attribution showing who used or owned the Device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, address books, contact lists, saved usernames and passwords, documents, and browsing history; and
 - k. Records evidencing the use of the Internet, including records of Internet Protocol addresses used;
2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT

for the
Western District of North CarolinaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

) Case No. 3:13-mj-99

The Premises Located at [REDACTED]
[REDACTED], as described in Affidavit
and Attachment, incorporated herein.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of North Carolina
(identify the person or describe the property to be searched and give its location):
See Attachment A, which is incorporated fully herein.The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):
See Attachment B, which is incorporated fully herein.I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.YOU ARE COMMANDED to execute this warrant on or before April 17, 2013

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____

Date and time issued:

4.3.13, 5:34pmRobert J. Conrad
Judge's signatureCity and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

Certified to be a true and
correct copy of the original.
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.
By B. F. Felling
Deputy Clerk
Date 4/4/13

Return

Case No.:

3:13mj 99

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature_____
Printed name and title

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Content of email account, as described in Affidavit and
Attachments, incorporated herein.

Case No. 3:13mj100

Certified to be a true and
correct copy of the original
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.
By: B. F. Fickling
Deputy Clerk
Date: 4/4/13

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of North Carolina
(identify the person or describe the property to be searched and give its location):
See Attachment A, which is incorporated fully herein.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):
See Attachment B, which is incorporated fully herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before April 17, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been
established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____

Date and time issued: 4.3.13, 5:30 p.m.

Robert J. Conrad, Jr.
Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

Return

Case No.: 3:13mj100	Date and time warrant executed:	Copy of warrant and inventory left with:
---------------------	---------------------------------	--

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature_____
Printed name and title

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

FILED
CHARLOTTE, NC

APR 4 2013

US District Court
Western District of NC

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 3:13-mj-100

Content of email account, as described in Affidavit and
Attachments, incorporated herein.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A, which is incorporated fully herein.

located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is incorporated fully herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 1924; 18 USC 793(e);	Unauthorized removal and retention of classified documents or material;
18 USC 371	Unauthorized possession, communication, and willful retention of national defense information; Conspiracy

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Certified to be a true and
correct copy of the original.
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.
By: B. Fickling
Deputy Clerk
Date: 4/4/13

Gerd J. Ballner
Applicant's signature

Gerd J. Ballner, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 04/03/2013

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr.
Judge's signature

Robert J. Conrad, Jr., United States District Court Judge
Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Gerd J. Ballner, Jr., being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account stored at premises owned, maintained, controlled, or operated by Yahoo! Inc., an email provider headquartered at 701 First Avenue, Sunnyvale, California 94089. The information to be searched is described in the following paragraphs and in Attachment A, all incorporated fully by reference herein.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for approximately thirteen years. I have investigated matters involving National Security to include Counterintelligence and Espionage. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by hostile foreign intelligence services and their recruited human sources to illegally obtain, through clandestine action, classified and proprietary information, which if compromised poses risk to the national security of the United States. I have also received specialized training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.
5. For the reasons set forth below, there is probable cause to believe that the email account [REDACTED] (described in detail in Attachment A) contains evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the improper communication and/or retention of classified information.
6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates,

delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.
9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."
10. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

11. David Petraeus is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about July 4, 2010 to July 18, 2011, Petraeus served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, Petraeus served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, Petraeus held a United States government security clearance allowing him access to classified United States government information. According to a Department of Defense (DOD) official, to obtain that clearance, Petraeus was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
12. [REDACTED] is a researcher and author of a biography of Petraeus, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. According to a DOD official, to obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
13. In June 2012, the FBI's Tampa Division (FBI Tampa) opened a computer intrusion investigation related to alleged cyber stalking activity. This investigation was predicated

on a complaint received from Witness 1, which alleged the receipt of threatening and harassing emails from the email addresses [REDACTED] and

[REDACTED] Witness 1 claimed friendships with several high-ranking public and military officials.

14. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of David Petraeus, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified Petraeus's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that Petraeus personally requested that Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that Petraeus believed the alleged cyber stalker possessed information which could "embarrass" Petraeus and other public officials.

15. Investigation conducted by FBI Tampa identified [REDACTED] as the person suspected of using the email accounts [REDACTED] and [REDACTED]. Investigation also determined [REDACTED] uses the email account [REDACTED]. On September 24, 2012, FBI Tampa interviewed [REDACTED] at her residence. During this interview [REDACTED] admitted sending the emails to Witness 1, as well as other emails regarding Witness 1 to senior United States military officers as well as a foreign diplomat. [REDACTED] also stated that she

engaged in an extramarital affair with Petraeus. [REDACTED] provided consent to search two of her laptop computers and two external hard drives.

16. On September 25, 2012, FBI Tampa returned [REDACTED] laptop computers and conducted a follow-up interview. During this follow-up interview, [REDACTED] admitted she told Petraeus that he should get Witness 1 to "drop the charges."

[REDACTED] advised she does not know if Petraeus made the request of Witness 1.

During the course of this interview, [REDACTED] provided interviewing agents consent to search her Apple iPhone, which she had in her possession. FBI Charlotte Computer Analysis Response Team (CART) Forensic Examiners copied the contents of her Apple iPhone at the interview location, and the iPhone was returned to [REDACTED] at the conclusion of the interview. A review of [REDACTED] laptops and external hard drives located over 100 items which were identified by Charlotte CART Forensic Examiners as containing potentially classified information, including information up to the Secret level.

17. On October 26, 2012, Petraeus was interviewed at CIA Headquarters. Petraeus stated that he had had an extramarital affair with [REDACTED]. He denied providing any classified documents to [REDACTED] or having any arrangement to provide her with classified information. Petraeus stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.

18. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about Petraeus; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from Petraeus.
19. During interviews conducted of [REDACTED] and Petraeus under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with one another. These methods included the use of pre-paid cellular telephones and email accounts using non-attributable names. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if all the accounts were identified because both [REDACTED] and Petraeus stated they could not recall all the account names which they created and used to communicate. During [REDACTED] September 25, 2012 interview, she advised that she and Petraeus would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

A. [REDACTED] Consensual Search, November 12, 2012

20. As a result of finding potentially classified information on the laptops provided by [REDACTED], FBI Tampa and FBI Charlotte conducted a consensual search of [REDACTED] Charlotte residence on November 12, 2012 to recover any evidence related to cyber stalking, in violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents or material, in violation of 18 U.S.C. § 1924. On this same date, a consensual search was also conducted at the residence of [REDACTED] administrative assistant, [REDACTED], in Concord, North Carolina. [REDACTED] voluntarily provided the FBI with various items she maintained in her home in relation to her employment with [REDACTED]. During the searches, additional paper documents were found, some of which, upon belief and information of your affiant, are classified. As a result of the two searches, the following digital media were seized: eight computers, twelve external hard drives, two printers/scanners, two cellular telephones, two Apple iPods, seven thumbdrives/memory cards, and approximately fifty floppy discs, CDs, and optical discs.
21. Based on a preliminary review of [REDACTED] digital media, it is believed she came into possession of potentially classified information both before and during the writing of her book, "All In: The Education of General David Petraeus." Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. Given her extensive use of digital media, your affiant believes [REDACTED] received/exchanged classified information via email and/or made contact with individuals via email and/or telephone to schedule in-person meetings for the purpose of recording and collecting classified information, as detailed below.

[REDACTED] is also believed to have digitally stored numerous documents, photographs, and audio interviews which contain classified information.

B. Relevant Communications Regarding the Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED] sent an email to Petraeus at email account [REDACTED]. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, the email related to a document or series of documents provided by Petraeus to [REDACTED] which contained classified information.¹

23. Between July 13, 2011 and July 15, 2011, [REDACTED] and a U.S. Army Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED] emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED] on July 15, 2011, he advised he was

¹ On June 27, 2012, FBI Tampa served a grand jury subpoena on Yahoo! for the [REDACTED] account. On June 29, 2012, FBI Tampa executed a search warrant on the account. On September 7, 2012, FBI Tampa obtained an additional search warrant on the account. Search warrant results received on October 16, 2012 included emails between the dates of July 1, 2012 and September 7, 2012. Because it is relevant to the current investigation what actions, if any, [REDACTED] took regarding the emails in the [REDACTED] account since the execution of the email search warrants by FBI Tampa, this affidavit seeks a search warrant requiring Yahoo! to disclose the entire contents of the account and not just the email content from September 7, 2012 to the present.

working on the storyboards and asked her for "a good SIPR number."² Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) Petraeus at email account [REDACTED]. [REDACTED] response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel reflects some agreement by Petraeus to provide [REDACTED] access to classified information.

24. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED], and Petraeus, using email address [REDACTED], discussed several topics, to include files maintained by Petraeus. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which Petraeus addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing Petraeus's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, Petraeus wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

² SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED] [REDACTED] the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there."³ In response Petraeus wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, Petraeus, using email address [REDACTED] and [REDACTED], using email address [REDACTED] exchanged over ten emails. In the first email, with the subject line "Found the", Petraeus discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED]. Petraeus wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about Petraeus's willingness to share the files writing: "[I]'ll protect them. And I'll protect you." Petraeus later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."⁴ Petraeus continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly

³ NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

⁴ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!**" (emphasis added).

27. Your affiant believes that Petraeus's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified.

C. Continuing Communications Between [REDACTED] and Petraeus

28. [REDACTED] and Petraeus are believed to have had multiple telephonic contacts after each was made aware of FBI Tampa's computer intrusion investigation. Your affiant asserts:
- a. Petraeus's CIA security detail was notified of the FBI investigation on June 22, 2012. In an interview with FBI Tampa on October 26, 2012, Petraeus acknowledged that: (1) he was briefed by the security detail concerning the FBI investigation, and (2) he called [REDACTED] on June 23, 2012 regarding the emails received by Witness 1.
 - b. Over the weekend of August 11, 2012 and August 12, 2012, Petraeus spoke to Witness 1. In evidence reviewed by FBI Charlotte, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on August 11, 2012.
 - c. [REDACTED] was interviewed by FBI Tampa on September 24, 25, and 26, 2012. A telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on three occasions on September 25, 2012.
 - d. [REDACTED] was in contact with FBI Tampa on October 1 and 2, 2012. These contacts ultimately resulted in a telephone interview conducted on October 3,

2012. In evidence reviewed by FBI Charlotte, on October 2, 2012, there were six calls between telephone numbers attributed to [REDACTED] and Petraeus. One of these calls connected, resulting in an approximately fifteen-minute-long conversation.

- e. During the October 26, 2012 interview of Petraeus by FBI Tampa, he stated that, while coming back from a trip to the Far East earlier in the month, he called [REDACTED], who told him about her interview with the FBI. Evidence indicated that a telephone number attributed to Petraeus called a telephone number attributed to [REDACTED] on October 16, 2012.
- f. Following FBI Tampa's interview of Petraeus on October 26, 2012, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on four occasions on October 27, 2012, on three occasions on October 28, 2012, and on two occasions on October 29, 2012.
- g. On November 2, 2012, [REDACTED] was again interviewed by FBI Tampa. [REDACTED] stated that she and Petraeus had talked candidly since each of their interviews with the FBI.
- h. On November 9, 2012, [REDACTED] contacted FBI Tampa telephonically from telephone number [REDACTED]. She advised she received a telephone call from Petraeus earlier that day advising her of his resignation. In evidence reviewed by FBI Charlotte, telephone number [REDACTED] called a telephone number attributed to Petraeus on November 9, 2012.

29. The foregoing telephone communications identified in this affidavit only include calls made or received from one government phone attributed to Petraeus. As detailed above,

Petraeus and [REDACTED] have previously been in regular contact through email, and communicated about the provision of classified information to [REDACTED]. Moreover, [REDACTED] and Petraeus have admitted that they established covert communications systems using pre-paid cellular telephones and non-attributable email accounts. To date, the pre-paid telephone numbers used by Petraeus and [REDACTED] have not been identified.

30. These telephonic contacts and attempted telephonic contacts between telephone numbers attributed to [REDACTED] and Petraeus indicate [REDACTED] relationship with Petraeus continued after their interviews with FBI Tampa in September and October 2012. Based on these facts, and given [REDACTED] history of email communication with Petraeus, there is probable cause to believe that [REDACTED] Yahoo! account contains substantive communications regarding the content of [REDACTED] and Petraeus's FBI interviews, including additional information regarding [REDACTED] access to and retention of classified information.

BACKGROUND CONCERNING EMAIL

31. In my training and experience, I have learned that Yahoo! provides a variety of online services, including electronic mail ("email") access, to the general public. Subscribers obtain an account by registering with Yahoo!. During the registration process, Yahoo! requests subscribers to provide basic personal information. Therefore, the computers of Yahoo! are likely to contain stored electronic communications (including retrieved and unretrieved email for Yahoo! subscribers) and information concerning subscribers and their use of Yahoo! services, such as account access information, email transaction information, and account application information. Such information can include the

subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

32. In general, an email that is sent to a Yahoo! subscriber is stored in the subscriber's "mail box" on Yahoo! servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Yahoo! servers indefinitely.
33. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Yahoo!'s servers, and then transmitted to its end destination. Yahoo! often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Yahoo! server, the email can remain on the system indefinitely.
34. A Yahoo! subscriber can also store files, including emails and other files, on servers maintained and/or owned by Yahoo!.
35. Subscribers to Yahoo! might not store on their home computers copies of the emails stored in their Yahoo! account. This is particularly true when they access their Yahoo! account through the web, or if they do not wish to maintain particular emails or files in their residence.
36. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods

used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

37. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

LOCATION TO BE SEARCHED

38. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Yahoo! to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Attachment A, the information described in Attachment B will be subject to seizure by law enforcement.

39. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information associated with a certain account, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by Yahoo! Inc., an email provider headquartered at 701 First Avenue, Sunnyvale, California 94089, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

CONCLUSION

40. Based on my training and experience, and the facts as set forth in this affidavit, your affiant asserts there is probable cause to believe that stored in the Yahoo! email account, [REDACTED] there exists evidence of a crime relating to: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

41. Based on the foregoing, I request that the Court issue the proposed search warrant.

Because the warrant will be served on Yahoo!, who will then compile the requested


records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

42. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by Title 18, United States Code, Section 2711; and Title 18, United States Code, Sections 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is “a district court of the United States that has jurisdiction over the offenses being investigated,” Title 18, United States Code, Sections 1924, 793(e), and 371. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

43. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

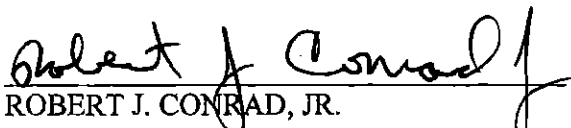
Respectfully submitted,



Gerd J. Ballner, Jr.
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me

on this, the 3 day of April, 2013.



ROBERT J. CONRAD, JR.
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A

Particular Account To Be Searched

This warrant applies to records and other information (including the contents of communications) for the account associated with the email address [REDACTED] that is stored at premises controlled by Yahoo!, a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California 94089.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed by Yahoo! ("the Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 16, 2012 and February 14, 2013, the Provider is required to disclose the following information to the government for the account listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information To Be Seized by the Government

1. All records or information described above in Section I that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant, including, for the account identified on Attachment A:

- a. All records or information related to any communications between [REDACTED] and Petraeus;
- b. All records or information related to any communications, from December 2008 to the present, between [REDACTED] and any other person or entity concerning classified and/or national defense information;
- c. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
- d. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED];
- e. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
- f. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

- g. All records or information related to any communications from June 2012 to the present between [REDACTED] and any other person concerning ongoing law enforcement investigations;
 - h. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by [REDACTED] or Petraeus;
 - i. Any information recording [REDACTED] or Petraeus's schedule or travel from December 2008 to the present;
 - j. Evidence of user attribution showing who used or owned the Device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, address books, contact lists, saved usernames and passwords, documents, and browsing history; and
 - k. Records evidencing the use of the Internet, including records of Internet Protocol addresses used;
- 2. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.
 - 3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT

for the
Western District of North CarolinaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Content of email accounts; forensic images of iPhone, 2
laptops, and 2 external hard drives, as described in
Affidavit and Attachment, incorporated herein.

Case No. 3:13mj/101

Certified to be a true and
correct copy of the original
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.By: B. Fickling
Deputy ClerkDate: 4/4/13

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of North Carolina
(Identify the person or describe the property to be searched and give its location):
See Attachment A, which is incorporated fully herein.The person or property to be searched, described above, is believed to conceal (Identify the person or describe the
property to be seized):
See Attachment B, which is incorporated fully herein.I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before

April 17, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m.☒ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____

Date and time issued:

4.3.13, 5:35 p.m.Robert J. Conrad
Judge's signatureCity and state: Charlotte, North CarolinaRobert J. Conrad, U.S. District Court Judge

Printed name and title

Return

Case No.:

3:13mj/61

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

UNITED STATES DISTRICT COURT

for the
Western District of North CarolinaFILED
CHARLOTTE, NC

APR 4 2013

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Content of email accounts; forensic images of iPhone, 2
laptops, and 2 external hard drives, as described in
Affidavit and Attachments, incorporated herein.US District Court
Western District of NC
Case No. 3:13-mj-10

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A, which is incorporated fully herein.located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):
See Attachment B, which is incorporated fully herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 1924; 18 USC 793(e);	Unauthorized removal and retention of classified documents or material;
18 USC 371	Unauthorized possession, communication, and willful retention of national defense information; Conspiracy

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Certified to be a true and
correct copy of the original
U.S. District Court
Frank G. Johns, Clerk
Western District of N.C.
By: B. Fickling
Deputy Clerk
Date: 4/4/13

111. DMJ
Applicant's signature

Gerd J. Ballner, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 04/03/2013

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr.
Judge's signature
Robert J. Conrad, Jr., United States District Court Judge
Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Gerd J. Ballner, Jr., being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with email accounts [REDACTED], [REDACTED], [REDACTED] and [REDACTED], as well as forensic images of an Apple iPhone (serial number C28J60GKDTDD), two laptop computers (Apple MacBook Air, serial number C02HF37GDJWV, and IBM/Lenova, serial number L3-AY867), and two external hard drives (Toshiba 500GB, serial number 523GFNJASN69, and LaCie, no visible serial number), which were previously searched and seized pursuant to search warrants or by consent during a computer intrusion investigation conducted by Federal Bureau of Investigation (FBI) Tampa Division.¹ All items are currently stored at the FBI Charlotte Field Office at 7915 Microsoft Way, Charlotte, North Carolina 28273. The items identified above are stored in a GSA-approved safe in a Sensitive Compartmented Information Facility, which is accessible only by FBI Charlotte Acting ASAC Scott Cheney, who is the designated filter agent on this investigation.² The specifics of the

¹ The following items were obtained by FBI Tampa by way of search warrants: email accounts [REDACTED], [REDACTED] and [REDACTED]

[REDACTED] The following items were obtained by FBI Tampa by way of consent: forensic images of an Apple iPhone (serial number C28J60GKDTDD), two laptop computers (Apple MacBook Air, serial number C02HF37GDJWV, and IBM/Lenova, serial number L3-AY867), and two external hard drives (Toshiba 500GB, serial number 523GFNJASN69, and LaCie, no visible serial number).

² The items which this affidavit seeks authority to search were originally seized, both pursuant to warrants and by way of consent, in a computer intrusion investigation by FBI Tampa. Those warrants did not permit the FBI to search for or seize items relating to the unlawful removal, communication, or storage of classified information, and the consent to search the laptop

information to be searched and items to be seized are more fully described in

Attachments A and B, which are incorporated fully by reference herein.

2. I am a Special Agent with the FBI and have been employed as such for approximately thirteen years. I have investigated matters involving National Security to include Counterintelligence and Espionage. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by hostile foreign intelligence services and their recruited human sources to illegally obtain, through clandestine action, classified and proprietary information, which if compromised poses grave danger to the national security of the United States. I have also received specialized training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

4. The FBI is conducting an investigation of [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and,

computers, external hard drives, and iPhone was obtained during the course of a voluntary interview focused on cyber stalking activities. The items have been stored by FBI Charlotte in the care of a filter agent. This filter agent has retained sole custody of the items to ensure no access to the information has been provided to agents investigating the matter under the statutes set forth in this affidavit.

inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.

5. For the reasons set forth below, there is probable cause to believe that the email accounts

██████████, ██████████, ██████████, and

██████████ as well as forensic images of an Apple iPhone (serial number C28J60GKDTDD), two laptop computers (Apple MacBook Air, serial number C02HF37GDJWV, and IBM/Lenova, serial number L3-AY867), and two external hard drives (Toshiba 500GB, serial number 523GFNJASN69, and LaCie, no visible serial number) contain evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful communication and/or retention of classified information. The items to be searched described in this paragraph consist entirely of items previously seized by the FBI pursuant to court authorized search warrants and by consent. All of the items remain in the FBI's possession. The prior search warrants allowed the FBI to search the items and seize materials relating to what was at the time an investigation into a potential cyber stalking matter, as more fully explained below. The instant request for a search warrant of those items is made to permit the FBI to search those items which are in the FBI's possession and seize materials relating to the violations set forth in paragraph 4 above. With regard to the email accounts identified above, the materials in the FBI's possession consist of data provided by internet service providers pursuant to service of the prior search warrants in the cyber stalking

investigation. The instant request is made to allow the FBI to search that data and seize those materials relating to violations set forth in paragraph 4 above.

6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.

9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original

classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."

10. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

11. David Petraeus is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, Petraeus served as Commander of the United States Central Command. From on or about July 4, 2010 to July 18, 2011, Petraeus served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, Petraeus served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, Petraeus held a United States government security clearance allowing him access to classified United States government information. According to a Department of Defense (DOD) official, to obtain that clearance, Petraeus was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to

receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

12. [REDACTED] is a researcher and author of a biography of Petraeus, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. According to a DOD official, to obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
13. In June 2012, the FBI's Tampa Division (FBI Tampa) opened a computer intrusion investigation related to alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1, which alleged the receipt of threatening and harassing emails from the email addresses [REDACTED] and [REDACTED]. Witness 1 claimed friendships with several high-ranking public and military officials.
14. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of Petraeus, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified Petraeus's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that Petraeus personally requested that

Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that Petraeus believed the alleged cyber stalker possessed information which could "embarrass" Petraeus and other public officials.

15. Investigation conducted by FBI Tampa identified [REDACTED] as the person suspected of using the email accounts [REDACTED] and [REDACTED] referred to above. Investigation also determined [REDACTED] used the email account [REDACTED] On September 24, 2012, FBI Tampa interviewed [REDACTED] at her residence. During this voluntary interview, [REDACTED] admitted sending the emails to Witness 1, as well as other emails regarding Witness 1 to senior United States military officers as well as a foreign diplomat. [REDACTED] also stated that she had engaged in an extramarital affair with Petraeus. [REDACTED] provided consent to search two of her laptop computers and two external hard drives. The computers were imaged by FBI Computer Analysis Response Team (CART) Forensic Examiners.

16. On September 25, 2012, FBI Tampa returned [REDACTED] laptop computers and conducted a follow-up interview. During this follow-up interview, [REDACTED] admitted she told Petraeus that he should get Witness 1 to "drop the charges." [REDACTED] advised agents that she did not know if Petraeus made the request of Witness 1. During the course of this interview, [REDACTED] provided interviewing agents consent to search her Apple iPhone, which she had in her possession. FBI CART

³ On June 29, 2012, FBI Tampa executed a search warrant on the [REDACTED] account. On September 7, 2012, FBI Tampa obtained an additional search warrant on the account. Search warrant results received on October 16, 2012 included emails between the dates of July 1, 2012 and September 7, 2012. On June 29, 2012, FBI Tampa executed a search warrant on the [REDACTED] account. On July 20, 2012, FBI Tampa executed a search warrant on the [REDACTED] account.

Forensic Examiners imaged the contents of her Apple iPhone at the interview location, and the iPhone was returned to [REDACTED], at the conclusion of the interview. A later review of [REDACTED]'s laptops and external hard drives located over 100 items which were identified by CART Forensic Examiners as containing potentially classified information, including information classified up to the Secret level.⁴

17. On October 26, 2012, Petraeus was interviewed at CIA Headquarters. Petraeus stated that he had had an extramarital affair with [REDACTED]. He denied providing any classified documents to [REDACTED] or having any arrangement to provide her with classified information. Petraeus stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.

18. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about Petraeus; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could

⁴ On September 26, 2012, FBI Tampa again met with [REDACTED] and returned the two external hard drives, which had also been imaged by CART Forensic Examiners.

not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book.

██████████, advised that she never received classified information from Petraeus.

19. During interviews conducted of ██████████ and Petraeus under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with one another. These methods included the use of pre-paid cellular telephones and email accounts using non-attributable names. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if all the accounts were identified because both ██████████ and Petraeus stated they could not recall all the account names which they created and used to communicate. During ██████████ September 25, 2012 interview, she advised that she and Petraeus would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

A. ██████████ Consensual Search, November 12, 2012

20. As a result of finding potentially classified information on the laptops provided by ██████████, FBI Tampa and FBI Charlotte conducted a consensual search of ██████████ Charlotte residence on November 12, 2012 to recover any evidence related to cyber stalking, in violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents or material, in violation of 18 U.S.C. § 1924. On this same date, a consensual search was also conducted at the residence of ██████████ administrative assistant, ██████████, in Concord, North Carolina. ██████████ voluntarily provided the FBI with various items she maintained in her home in relation to her employment with ██████████. During the searches,

additional paper documents were found, some of which, upon belief and information of your affiant, are classified. As a result of the two searches, the following digital media were seized: eight computers, twelve external hard drives, two printers/scanners, two cellular telephones, two Apple iPods, seven thumbdrives/memory cards, and approximately fifty floppy discs, CDs, and optical discs.⁵

21. Based on a preliminary review of [REDACTED] digital media, it is believed she came into possession of potentially classified information both before and during the writing of her book, "All In: The Education of General David Petraeus." Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. Given her extensive use of digital media, your affiant believes [REDACTED] received/exchanged classified information via email and/or made contact with individuals via email and/or telephone to schedule in-person meetings for the purpose of recording and collecting classified information, as detailed below.
- [REDACTED] is also known to have digitally stored numerous documents, photographs, and audio interviews which contain classified information.

B. Communications Regarding the Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED] sent an email to Petraeus at email account [REDACTED]. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parentheses, or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, the email related to a

⁵ These items include the two laptops and two external hard drives previously provided by [REDACTED] to FBI on September 24, 2012.

document or series of documents provided by Petraeus to [REDACTED] which contained classified information.

23. Between July 13, 2011 and July 15, 2011, [REDACTED] and a U.S. Army Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED] emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED] on July 15, 2011, he advised he was working on the storyboards and asked her for "a good SIPR number."⁶ Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) Petraeus at email account [REDACTED]. [REDACTED] response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel reflects some agreement by Petraeus to provide [REDACTED] access to classified information.

24. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED] and Petraeus, using email address [REDACTED], discussed several topics, to include files

⁶ SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

maintained by Petraeus. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which Petraeus addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing Petraeus's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, Petraeus wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED] [REDACTED], the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there."⁷ In response Petraeus wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, Petraeus, using email address [REDACTED] and [REDACTED] using email address [REDACTED], exchanged over ten emails. In the first email, with the subject line "Found the", Petraeus discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED]. Petraeus wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about Petraeus's willingness to share the files writing: "[I]'ll protect them. And I'll protect you." Petraeus later responded to

⁷ NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

██████████, writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."⁸ Petraeus continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if ██████████ kept copies. **Class'd, but I guess I might share!**" (emphasis added).

27. Your affiant believes that Petraeus's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to ██████████, --- are classified.

C. Continuing Communications Between ██████████ and Petraeus

28. ██████████ and Petraeus are believed to have had multiple telephonic contacts after each was made aware of FBI Tampa's computer intrusion investigation. Your affiant asserts:

- a. Petraeus's CIA security detail was notified of the FBI investigation on June 22, 2012. In an interview with FBI Tampa on October 26, 2012, Petraeus acknowledged that: (1) he was briefed by the security detail concerning the FBI investigation, and (2) he called ██████████ on June 23, 2012 regarding the emails received by Witness 1.

⁸ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

- b. Over the weekend of August 11, 2012 and August 12, 2012, Petraeus spoke to Witness 1. In evidence reviewed by FBI Charlotte, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on August 11, 2012.
- c. [REDACTED] was interviewed by FBI Tampa on September 24, 25, and 26, 2012. A telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on three occasions on September 25, 2012.
- d. [REDACTED] was in contact with FBI Tampa on October 1 and 2, 2012. These contacts ultimately resulted in a telephone interview conducted on October 3, 2012. In evidence reviewed by FBI Charlotte, on October 2, 2012, there were six calls between telephone numbers attributed to [REDACTED] and Petraeus. One of these calls connected, resulting in an approximately fifteen-minute-long conversation.
- e. During the October 26, 2012 interview of Petraeus by FBI Tampa, he stated that, while coming back from a trip to the Far East earlier in the month, he called [REDACTED], who told him about her interview with the FBI. Evidence indicated that a telephone number attributed to Petraeus called a telephone number attributed to [REDACTED] on October 16, 2012.
- f. Following FBI Tampa's interview of Petraeus on October 26, 2012, a telephone number attributed to [REDACTED] called a telephone number attributed to Petraeus on four occasions on October 27, 2012, on three occasions on October 28, 2012, and on two occasions on October 29, 2012.

g. On November 2, 2012, [REDACTED] was again interviewed by FBI Tampa.

[REDACTED] stated that she and Petraeus had talked candidly since each of their interviews with the FBI.

h. On November 9, 2012, [REDACTED] contacted FBI Tampa telephonically from telephone number [REDACTED]. She advised she received a telephone call from Petraeus earlier that day advising her of his resignation. In evidence reviewed by FBI Charlotte, telephone number [REDACTED] called a telephone number attributed to Petraeus on November 9, 2012.

29. The foregoing telephone communications identified in this affidavit only include calls made or received from one government phone attributed to Petraeus. As detailed above, Petraeus and [REDACTED] have previously been in regular contact through email, and communicated about the provision of classified information to [REDACTED]. Moreover, [REDACTED] and Petraeus have admitted that they established covert communications systems using pre-paid cellular telephones and non-attributable email accounts. One of the non-attributable email accounts used by [REDACTED] was [REDACTED].⁹ To date, the pre-paid telephone numbers used by Petraeus and [REDACTED] have not been identified.

30. These telephonic contacts and attempted telephonic contacts between telephone numbers attributed to [REDACTED] and Petraeus indicate [REDACTED] relationship with Petraeus continued after their interviews with FBI Tampa in September and October 2012. Based on these facts, and given [REDACTED] history of email communication with Petraeus, there is probable cause to believe that the [REDACTED]

⁹ On September 5, 2012, FBI Tampa executed a search warrant on the [REDACTED] account.

account as well as the [REDACTED] account contain substantive communications regarding the content of [REDACTED] and Petraeus's FBI interviews, including additional information regarding [REDACTED] access to and retention of classified information.

LOCATION TO BE SEARCHED

31. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant to search the evidence previously seized by FBI Tampa, to include email accounts: [REDACTED], [REDACTED], [REDACTED], and [REDACTED] as well as forensic images of an iPhone (serial number C28J60GKDTDD), two laptop computers (Apple MacBook Air, serial number C02HF37GDJWV, and IBM/Lenova, serial number L3-AY867), and two external hard drives (Toshiba 500GB, serial number 523GFNJASN69, and LaCie, no visible serial number), all of which are stored at the FBI Charlotte Field Office at 7915 Microsoft Way, Charlotte, North Carolina 28273. The items are stored in a GSA-approved safe in a Sensitive Compartmented Information Facility, which is accessible only by Acting ASAC Scott Cheney, the designated filter agent in the investigation.

CONCLUSION

32. Based on my training and experience, and the facts as set forth in this affidavit, your affiant asserts there is probable cause to believe that within the aforementioned items there exists evidence of a crime relating to: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, *inter alia*, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful

retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

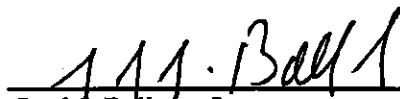
33. Based on the foregoing, I request that the Court issue the proposed search warrant.

Because the warrant will be served on the Federal Bureau of Investigation, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

34. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.


Respectfully submitted,



Gerd J. Ballner, Jr.
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me

on this, the 3d day of April, 2013.



ROBERT J. CONRAD, JR.
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A

Particular Items To Be Searched

This warrant applies to records and other information contained within evidence seized by FBI Tampa pursuant to warrants or by consent in a computer intrusion investigation of

██████████ to include:

1. Content of email account ██████████ received by FBI Tampa pursuant to search warrants executed on June 29, 2012 and September 7, 2012;
2. Content of email account ██████████ received by FBI Tampa pursuant to a search warrant executed September 5, 2012;
3. Content of email account ██████████ received by FBI Tampa pursuant to a search warrant executed June 29, 2012;
4. Content of email account ██████████ received by FBI Tampa pursuant to a search warrant executed July 20, 2012;
5. Forensic image of an Apple iPhone, serial number C28J60GKDTDD, obtained by consent on September 25, 2012;
6. Forensic image of an Apple MacBook Air laptop computer, serial number C02HF37GDJWV, obtained by consent on September 24, 2012;
7. Forensic image of an IBM/Lenova laptop computer, serial number L3-AY867, obtained by consent on September 24, 2012;
8. Forensic image of a Toshiba 500GB external hard drive, serial number 523GFNJASN69, obtained by consent on September 24, 2012; and
9. Forensic image of a LaCie external hard drive, no visible serial number, obtained by consent on September 24, 2012;

all of which are stored in a GSA-approved safe in a Sensitive Compartmented Information Facility located at the FBI Charlotte Field Office at 7915 Microsoft Way, Charlotte, North Carolina 28273.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Seized by the Government

1. All records or information that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant, including:
 - a. All records or information related to any communications between [REDACTED] and Petraeus;
 - b. All records or information related to any communications, from December 2008 to the present, between [REDACTED] and any other person or entity concerning classified and/or national defense information;
 - c. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
 - d. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided to [REDACTED] and any involvement of Petraeus in such;
 - e. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
 - f. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

- g. All records or information related to any communications from June 2012 to the present between [REDACTED] and any other person concerning ongoing law enforcement investigations;
- h. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by [REDACTED] or Petraeus;
- i. Any information recording [REDACTED] or Petraeus's schedule or travel from December 2008 to the present; and
- j. Records evidencing the use of the Internet, including records of Internet Protocol addresses used;

- 2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

FILED
CHARLOTTE, NC

AUG - 8 2013

UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

US District Court
Western District of NCIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Content and forensic images of email account as
described in Affidavit and Attachment, incorporated
herein.

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A, which is incorporated fully herein.

located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See attachment B which is incorporated fully herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 1924	Unauthorized removal and retention of classified documents and materials.
18 U.S.C. 793(e)	Unauthorized possession, communication and willful retention of national defense information

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Raju S. Bhatia

Applicant's signature

Raju S. Bhatia Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

8.8.13

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr.

Judge's signature

Robert J. Conrad, Jr., United States District Court Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Raju S. Bhatia, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account stored at premises owned, maintained, controlled, or operated by United States Central Command (US CENTCOM) headquartered at MacDill Air Force Base, Tampa, Florida. The information to be searched is described in the following paragraphs and in Attachment A, all incorporated fully by reference herein.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for over 14 years. I have investigated matters involving complex financial fraud, public corruption, organized crime, counterterrorism, and counterespionage. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by individuals attempting to conceal their illegal behavior. I have also received training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.
5. For the reasons set forth below, there is probable cause to believe that the email account [REDACTED] (described in detail in Attachment A) contains evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the improper communication and/or retention of classified information.
6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).
7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates,

delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.
9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."
10. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

11. PETRAEUS is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about June 23, 2010 to July 18, 2011, PETRAEUS served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, PETRAEUS served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, PETRAEUS held a United States government security clearance allowing him access to classified United States government information. To obtain that clearance, PETRAEUS was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
12. [REDACTED] is a researcher and author of a biography of PETRAEUS, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. To obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
13. In June 2012, the FBI's Tampa Division (FBI Tampa) opened a computer intrusion investigation related to alleged cyber stalking activity. This investigation was predicated

on a complaint received from Witness 1, which alleged the receipt of threatening and harassing emails. Witness 1 claimed friendships with several high-ranking public and military officials.

14. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of PETRAEUS, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified PETRAEUS's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that PETRAEUS personally requested that Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that PETRAEUS believed the alleged cyber stalker possessed information which could "embarrass" PETRAEUS and other public officials. Ultimately the FBI determined, based upon the investigation, that

██████████ was the individual who had sent the emails to Witness 1.

15. On September 24, 2012 as part of the FBI Tampa investigation, ██████████ consented to a search of two laptops and two external hard drives belonging to her. A review of the digital media contained on these devices revealed over 100 items which were identified by Charlotte Computer Analysis Response Team (CART) Forensic Examiners as potentially containing classified information, up to the Secret level.
16. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with ██████████. He denied providing any classified documents to ██████████ or having any arrangement to provide her

with classified information. PETRAEUS stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.

17. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from PETRAEUS.

18. During interviews conducted of [REDACTED] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of pre-paid cellular telephones and email accounts using non-attributable names. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not

known if all the accounts were identified because both [REDACTED] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [REDACTED] September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

19. On November 12, 2012, Agents from the Charlotte and Tampa Divisions of the FBI participated in a consensual search of [REDACTED] residence in [REDACTED], North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital media as well as four boxes and one folder of documents. On this same date, [REDACTED] administrative assistant voluntarily provided the FBI with digital media as well as one box of documents which she maintained in her home in relation to her employment with [REDACTED]. A review of the seized materials has identified to date hundreds of potentially classified documents, including more than 300 marked Secret, on digital images maintained on various pieces of electronic media.
20. Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. [REDACTED] traveled into and out of Afghanistan several times between September 2010 and July 2011 to conduct research for a biography on PETRAEUS. During this time, PETRAEUS was serving as the International Security Assistance Force (ISAF) Commander.
21. [REDACTED] paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting [REDACTED] access to classified information for the

purpose of writing his biography. For example, in an email dated January 16, 2011, which PETRAEUS marked as CONFIDENTIAL and sent to multiple members of the military, he instructed a member of his staff to "PLS PRINT FOR [REDACTED], ON AN OFF THE RECORD BASIS." Travel documents show that [REDACTED] was in Afghanistan at this time.

A. Communications Regarding Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED] sent an email to PETRAEUS at email account [REDACTED]. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, the email related to a document or series of documents provided by PETRAEUS to [REDACTED] which contained classified information.
23. Between July 13, 2011 and July 15, 2011, [REDACTED] and a U.S. Army Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED] emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED] on July 15, 2011, he advised he was

working on the storyboards and asked her for "a good SIPR number."¹ Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) PETRAEUS at email account [REDACTED] [REDACTED] response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

24. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED] and PETRAEUS, using email address [REDACTED], discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which PETRAEUS addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing PETRAEUS's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

¹ SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! Susan Lemke, the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there."² In response, PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address

[REDACTED], and [REDACTED], using email address

[REDACTED] exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED].

PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about PETRAEUS's willingness to share the files writing: "[I]'ll protect them. And I'll protect you."

PETRAEUS later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."³ PETRAEUS continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to

² NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

³ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!"** (Emphasis added).

27. Your affiant believes that PETRAEUS's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified.

28. Based on these facts, there is probable cause to believe that PETRAEUS's email account, [REDACTED], contains substantive communications regarding PETRAEUS's sharing of classified information as well as [REDACTED] access to and retention of classified information.

BACKGROUND CONCERNING EMAIL

29. In my training and experience, I have learned that US CENTCOM provides electronic mail ("email") access to uniformed and civilian employees. These users are provided an email account for use in their official duties. Consequently, US CENTCOM computers are likely to contain stored electronic communications (including retrieved and unretrieved email for US CENTCOM users) and information concerning users and their use of US CENTCOM services. This information would include details regarding users of US CENTCOM service, such as the user's full name, physical locations, telephone numbers and other identifiers, account access information, email transaction information, and alternative email addresses. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

30. In general, an email that is sent to a CENTCOM subscriber is stored in the subscriber's "mail box" on CENTCOM servers until the subscriber deletes the email. If the

subscriber does not delete the message, the message can remain on CENTCOM servers indefinitely.

31. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to CENTCOM servers, and then transmitted to its end destination.

CENTCOM often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the CENTCOM server, the email can remain on the system indefinitely.

32. A CENTCOM subscriber can also store files, including emails, files and other data, on servers maintained and/or owned by CENTCOM.

33. Subscribers to CENTCOM might not store, on their home computers, copies of the emails stored in their CENTCOM account. This is particularly true when the subscriber accesses their CENTCOM account through the web, or if they do not maintain particular emails or files in their residence or on their home computer.

34. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information

can help to identify which computers or other devices were used to access the email account.

35. In my training and experience, in some cases email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

LOCATION TO BE SEARCHED

36. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the requested warrant to require US CENTCOM to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Attachment A, the information described in Attachment B will be subject to seizure by law enforcement.
37. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information associated with a certain account, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by US CENTCOM, headquartered at MacDill Air Force Base, Tampa, Florida, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized

possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

CONCLUSION

38. Based on my training and experience, and the facts as set forth in this affidavit, your affiant asserts there is probable cause to believe that stored in the email account, [REDACTED], there exists evidence of a crime relating to: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.
39. Based on the foregoing, I request that the Court issue the requested search warrant. Because the warrant will be served on US CENTCOM, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.
40. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, United States Code, Section 2711; and Title 18, United States Code, Sections 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offenses being

investigated," Title 18, United States Code, Sections 1924, 793(e), and 371. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

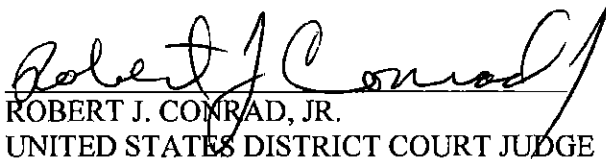
41. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Respectfully submitted,



Raju S. Bhatia
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this, the 8th day of August, 2013.




ROBERT J. CONRAD, JR.
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A

Particular Account To Be Searched

This warrant applies to records and other information (including the contents of communications) for the account associated with the email address

 that is stored at premises controlled by US Central Command, which accepts service of legal process at MacDill Air Force Base, Tampa, Florida.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed by CENTCOM ("the Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the account listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, and log files;
- c. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- d. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information To Be Seized by the Government

1. All records or information described above in Section I that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant, including, for the account identified on Attachment A:
 - a. All records or information related to any communications between PETRAEUS and [REDACTED];
 - b. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;
 - c. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
 - d. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided by PETRAEUS to [REDACTED];
 - e. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
 - f. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;
 - g. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;

- h. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS or [REDACTED];
 - i. Any information recording PETRAEUS's or [REDACTED] schedule or travel from December 2008 to the present;
and
 - j. Records evidencing the use of the Internet, including records of Internet Protocol addresses used;
- 2. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.
- 3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

FILED
CHARLOTTE, NC

AUG - 8 2013

US District Court
Western District of NC

UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Content and forensic images of email account as
described in Affidavit and Attachment, incorporated
herein.

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A, which is incorporated fully herein.

located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See attachment B which is incorporated fully herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. 1924
 18 U.S.C. 793(e)

Offense Description
 Unauthorized removal and retention of classified documents and materials.
 Unauthorized possession, communication and willful retention of national defense information

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Raju S. Bhatia

Applicant's signature

Raju S. Bhatia Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

8.8.13

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr.

Judge's signature

Robert J. Conrad, Jr., United States District Court Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Raju S Bhatia, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain email account stored at premises owned, maintained, controlled, or operated by United States Central Command (US CENTCOM) headquartered at MacDill Air Force Base, Tampa, Florida. The information to be searched is described in the following paragraphs and in Attachment A, all incorporated fully by reference herein.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for over 14 years. I have investigated matters involving complex financial fraud, public corruption, organized crime, counterterrorism, and counterespionage. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by individuals attempting to conceal their illegal behavior. I have also received training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.

5. For the reasons set forth below, there is probable cause to believe that the email account [REDACTED] (described in detail in Attachment A) contains evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the improper communication and/or retention of classified information.

6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates,

delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.
9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."
10. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

11. PETRAEUS is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about June 23, 2010 to July 18, 2011, PETRAEUS served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, PETRAEUS served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, PETRAEUS held a United States government security clearance allowing him access to classified United States government information. To obtain that clearance, PETRAEUS was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
12. [REDACTED] is a researcher and author of a biography of PETRAEUS, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. To obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
13. In June 2012, the FBI's Tampa Division (FBI Tampa) opened a computer intrusion investigation related to alleged cyber stalking activity. This investigation was predicated

on a complaint received from Witness 1, which alleged the receipt of threatening and harassing. Witness 1 claimed friendships with several high-ranking public and military officials.

14. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of PETRAEUS, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified PETRAEUS's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that PETRAEUS personally requested that Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that PETRAEUS believed the alleged cyber stalker possessed information which could "embarrass" PETRAEUS and other public officials. Ultimately the FBI determined, based upon the investigation, that

██████████ was the individual who had sent the emails to Witness 1.

15. On September 24, 2012 as part of the FBI Tampa investigation, ██████████ consented to a search of two laptops and two external hard drives belonging to her. A review of the digital media contained on these devices revealed over 100 items which were identified by Charlotte Computer Analysis Response Team (CART) Forensic Examiners as potentially containing classified information, up to the Secret level.
16. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with ██████████. He denied providing any classified documents to ██████████ or having any arrangement to provide her

with classified information. PETRAEUS stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.

17. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from PETRAEUS.

18. During interviews conducted of [REDACTED] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of email accounts using non-attributable names and pre-paid cellular telephones. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if

all the accounts were identified because both [REDACTED] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [REDACTED] September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

19. On November 12, 2012, Agents from the Charlotte and Tampa Divisions of the FBI participated in a consensual search of [REDACTED] residence in Charlotte, North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital media as well as four boxes and one folder of documents. On this same date, [REDACTED] administrative assistant voluntarily provided the FBI with digital media as well as one box of documents which she maintained in her home in relation to her employment with [REDACTED]. A review of the seized materials has identified to date hundreds of potentially classified documents, including more than 300 marked Secret, on digital images maintained on various pieces of electronic media.

20. Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. [REDACTED] traveled into and out of Afghanistan several times between September 2010 and July 2011 to conduct research for a biography on PETRAEUS. During this time, PETRAEUS was serving as the International Security Assistance Force (ISAF) Commander.

21. [REDACTED] paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting [REDACTED] access to classified information for the purpose of writing his biography.

A. Communications Regarding Potential Mishandling of Classified Information

22. On December 29, 2009, PETRAUES, using email account [REDACTED], sent an email to [REDACTED] at email account [REDACTED]. During a series of emails with the subject line, "Lincoln's T-Mails?" PETRAUES wrote to [REDACTED], "You're pretty accurate! Off in the morning to Iraq, Sinai, and possibly the new focus of our attention..." Based on my training, experience, and information reviewed to date in this investigation, PETRAUES routinely provided [REDACTED] with his schedule and potentially classified operational plans.
23. On January 14, 2010, [REDACTED], using email account [REDACTED], sent an email to PETRAEUS at email account [REDACTED]. The subject line of the email read: "Revolutions in Doctrine" and the body of the email read: "Thank you for this rich feedback. Again, I appreciate your candor! (Except when the off-the-record stuff is so important but I can't use it for PC reasons...damn☺)"
24. On January 16, 2010, [REDACTED], using email account [REDACTED], sent an email to PETRAEUS at email account [REDACTED]. The body of the email read, "GEN Petraeus, The research hat is back on! These attached are some good emails too. Mostly, all of these provide a wonderful timeline of key domestic and Iraq events and your associated sentiment at the time. Thank goodness and lucky me! Good see rapprochement between you and then candidate Obama. (I'm curious about

your promise to tell [REDACTED] about the "one-on-one" discussion you had. Dare I ask?) And I know enough to keep your discussions about politicians with [REDACTED] OTR ...

PETRAEUS replied to [REDACTED], "I'll tell you my pull-aside with now POTUS someday. I owed it to him and was a bit astonished at the self-confidence of his reply- but also quite reassured."

25. On January 23, 2010, [REDACTED], using email account [REDACTED] sent an email to PETRAEUS at email account [REDACTED]. The body of the email read, "GEN Petraeus, Please tell me about your conversation with PM TB! ☺ Best [REDACTED]" Based on the investigation to date, "PM TB" is believed to be then-British Prime Minister Tony Blair. PETRAEUS replied to [REDACTED], "☺" to which [REDACTED] wrote, "pretty please? ☺" PETRAEUS responded, "Add it to the 'over a beer' list, pls. [REDACTED].."

26. Based on my training, experience, and information reviewed to date in this investigation, the emails referenced in paragraphs 23, 24, and 25 demonstrate PETRAEUS' willingness to provide sensitive information to [REDACTED], on an "off the record" basis.

27. On January 16, 2010, PETRAEUS, using email account [REDACTED] forwarded an email to [REDACTED] at email account [REDACTED]. The forwarded email stated, "[REDACTED] the exchanges you've had with [REDACTED] reminded me of the courage you showed in writing your 'strategic Op-Ed' piece in July 07...I think you need to do another one today... The situation in Iraq has turned very serious in the past 48-72 hours with the Accountability and Justice Commission (run by Faisal al-Lami, an Iranian controlled individual, who's being guided by Ahmed Chalabi) recommending over 400 candidates for the Parliamentary Elections be disqualified..." PETRAEUS was

worried about the results of this process and its implications for Iraq. PETRAEUS continued, writing, "We need to galvanize national/world attention/pressure" and ended by saying "Pls protect your source as always. Best – Dave" In her response to PETRAEUS' forwarded email, [REDACTED] wrote, "He is flying to Florida today with his parents...I know I am nobody but let me know if I can help!"

28. PETRAEUS followed up shortly with an email from his [REDACTED] email account to a British political advisor at another CENTCOM-based email account. In the email to the British political advisor PETRAEUS wrote, "ok, please don't betray my hand (act surprised with [REDACTED]), but think this is a way of getting attention to this crisis. I shot up a big red star cluster on SIPR last night too. Got attention. Alerted WH and SEN McCain, as well. Again, please don't share with other than the big one (but tell him). We need to save our beloved land of the two rivers..."

29. [REDACTED] had a copy of the email exchange referenced in paragraphs 27 and 28 in her [REDACTED] email account. Based on information reviewed to date in this investigation, it is believed that PETRAEUS blind carbon copied (bcc) [REDACTED] on many of his email exchanges, and the email above appears to have been found in [REDACTED] Yahoo! Account because she was bcc'd by PETRAEUS.

30. Based on my training, experience, and information reviewed to date in this investigation, the emails referenced in paragraphs 27 and 28 demonstrate PETRAEUS' willingness to share and provide access to sensitive and possibly classified material with [REDACTED].

31. Based on these facts, and given PETRAEUS's history of email communication with [REDACTED], there is probably cause to believe that PETRAEUS's email account,

[REDACTED], contains substantive communications regarding
[REDACTED] access to and retention of classified information.

BACKGROUND CONCERNING EMAIL

32. In my training and experience, I have learned that US CENTCOM provides electronic mail ("email") access to uniformed and civilian employees. These users are provided an email account for use in their official duties. Consequently, US CENTCOM computers are likely to contain stored electronic communications (including retrieved and unretrieved email for US CENTCOM users) and information concerning users and their use of US CENTCOM services. This information would include details regarding users of US CENTCOM service, such as the user's full name, physical locations, telephone numbers and other identifiers, account access information, email transaction information, and alternative email addresses. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
33. In general, an email that is sent to a CENTCOM subscriber is stored in the subscriber's "mail box" on CENTCOM servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on CENTCOM servers indefinitely.
34. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to CENTCOM servers, and then transmitted to its end destination. CENTCOM often saves a copy of the email sent. Unless the sender of the email

specifically deletes the email from the CENTCOM server, the email can remain on the system indefinitely.

35. A CENTCOM subscriber can also store files, including emails, files and other data, on servers maintained and/or owned by CENTCOM.
36. Subscribers to CENTCOM might not store, on their home computers, copies of the emails stored in their CENTCOM account. This is particularly true when the subscriber accesses their CENTCOM account through the web, or if they do not maintain particular emails or files in their residence or on their home computer.
37. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.
38. In my training and experience, in some cases email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers

typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

LOCATION TO BE SEARCHED

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the requested warrant to require US CENTCOM to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Attachment A, the information described in Attachment B will be subject to seizure by law enforcement.
40. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information associated with a certain account, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by US CENTCOM, headquartered at MacDill Air Force Base, Tampa, Florida, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

CONCLUSION

41. Based on my training and experience, and the facts as set forth in this affidavit, your affiant asserts there is probable cause to believe that stored in the US CENTCOM email account, [REDACTED], there exists evidence of a crime relating to: a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

42. Based on the foregoing, I request that the Court issue the requested search warrant.


Because the warrant will be served on US CENTCOM, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

43. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, United States Code, Section 2711; and Title 18, United States Code, Sections 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offenses being investigated," Title 18, United States Code, Sections 1924, 793(e), and 371. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING


44. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Respectfully submitted,



Raju S. Bhatia
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this, the 28th day of August, 2013.



ROBERT J. CONRAD, JR.
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A

Particular Account To Be Searched

This warrant applies to records and other information (including the contents of communications) for the account associated with the email address [REDACTED] that is stored at premises controlled by US Central Command, which accepts service of legal process at MacDill Air Force Base, Tampa, Florida.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed by CENTCOM ("the Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the account listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information To Be Seized by the Government

1. All records or information described above in Section I that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant, including, for the account identified on Attachment A:
 - a. All records or information related to any communications between PETRAEUS and [REDACTED];
 - b. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;
 - c. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
 - d. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided by PETRAEUS to [REDACTED];
 - e. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
 - f. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;
 - g. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;

- h. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS or [REDACTED];
 - i. Any information recording PETRAEUS's or [REDACTED] schedule or travel from December 2008 to the present;
 - j. Evidence of user attribution showing who used or owned the Device at the time the items described in this warrant were created, edited, or deleted, such as logs, phonebooks, address books, contact lists, saved usernames and passwords, documents, and browsing history; and
 - k. Records evidencing the use of the Internet, including records of Internet Protocol addresses used;
2. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.
3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT

FILED
CHARLOTTE, NC

for the

Western District of North Carolina

AUG - 8 2013

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Content and forensic images of email account as
described in Affidavit and Attachment, incorporated
herein.

Case No.

US District Court
Western District of NC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A, which is incorporated fully herein.

located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See attachment B which is incorporated fully herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. 1924
 18 U.S.C. 793(e)

Offense Description
 Unauthorized removal and retention of classified documents and materials.
 Unauthorized possession, communication and willful retention of national defense information

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

(SA) Raju S. Bhatia
 Applicant's signature

Raju S. Bhatia Special Agent, FBI
 Printed name and title

Sworn to before me and signed in my presence.

Date: 8.8.13

City and state: Charlotte, North Carolina

Robert J. Conrad, Jr.
 Judge's signature
 Robert J. Conrad, Jr., United States District Court Judge
 Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Raju S Bhatia, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account stored at premises owned, maintained, controlled, or operated by United States Central Command (US CENTCOM) headquartered at MacDill Air Force Base, Tampa, Florida. The information to be searched is described in the following paragraphs and in Attachment A, all incorporated fully by reference herein.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for over 14 years. I have investigated matters involving complex financial fraud, public corruption, organized crime, counterterrorism, and counterespionage. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by individuals attempting to conceal their illegal behavior. I have also received training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.
5. For the reasons set forth below, there is probable cause to believe that the email account [REDACTED] (described in detail in Attachment A) contains evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the improper communication and/or retention of classified information.
6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).
7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates,

delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.
9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."
10. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

11. PETRAEUS is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about June 23, 2010 to July 18, 2011, PETRAEUS served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, PETRAEUS served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, PETRAEUS held a United States government security clearance allowing him access to classified United States government information. To obtain that clearance, PETRAEUS was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
12. [REDACTED] is a researcher and author of a biography of PETRAEUS, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. To obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
13. In June 2012, the FBI's Tampa Division (FBI Tampa) opened a computer intrusion investigation related to alleged cyber stalking activity. This investigation was predicated

on a complaint received from Witness 1, which alleged the receipt of threatening and harassing emails. Witness 1 claimed friendships with several high-ranking public and military officials.

14. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of PETRAEUS, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified PETRAEUS's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that PETRAEUS personally requested that Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that PETRAEUS believed the alleged cyber stalker possessed information which could "embarrass" PETRAEUS and other public officials. Ultimately the FBI determined, based upon the investigation, that

██████████ was the individual who had sent the emails to Witness 1.

15. On September 24, 2012 as part of the FBI Tampa investigation, ██████████ consented to a search of two laptops and two external hard drives belonging to her. A review of the digital media contained on these devices revealed over 100 items which were identified by Charlotte Computer Analysis Response Team (CART) Forensic Examiners as potentially containing classified information, up to the Secret level.
16. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with ██████████. He denied providing any classified documents to ██████████ or having any arrangement to provide her

with classified information. PETRAEUS stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.

17. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from PETRAEUS.

18. During interviews conducted of [REDACTED] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of pre-paid cellular telephones and email accounts using non-attributable names. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not

known if all the accounts were identified because both [REDACTED] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [REDACTED] September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

19. On November 12, 2012, Agents from the Charlotte and Tampa Divisions of the FBI participated in a consensual search of [REDACTED] residence in [REDACTED], North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital media as well as four boxes and one folder of documents. On this same date, [REDACTED] administrative assistant voluntarily provided the FBI with digital media as well as one box of documents which she maintained in her home in relation to her employment with [REDACTED]. A review of the seized materials has identified to date hundreds of potentially classified documents, including more than 300 marked Secret, on digital images maintained on various pieces of electronic media.
20. Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. [REDACTED] traveled into and out of Afghanistan several times between September 2010 and July 2011 to conduct research for a biography on PETRAEUS. During this time, PETRAEUS was serving as the International Security Assistance Force (ISAF) Commander.
21. [REDACTED] paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting [REDACTED] access to classified information for the

purpose of writing his biography. For example, in an email dated January 16, 2011, which PETRAEUS marked as CONFIDENTIAL and sent to multiple members of the military, he instructed a member of his staff to "PLS PRINT FOR [REDACTED], ON AN OFF THE RECORD BASIS." Travel documents show that [REDACTED] was in Afghanistan at this time.

A. Communications Regarding Potential Mishandling of Classified Information

22. On July 13, 2011, [REDACTED] and a U.S. Army Captain exchanged several emails. [REDACTED], using email account [REDACTED] emailed the Captain at his military email account, seeking information about military operations. In an email to the Captain, in which PETRAEUS was carbon copied (cc'd) at email account [REDACTED], [REDACTED] wrote, "If it's ok with you, may I trouble you to send the storyboards (via SIPR¹) directly to GEN Petraeus (copied here) and he will print them out for me? (He is gracious and willing to help out given my compressed timeline!)" PETRAEUS followed up to this email by writing to the Captain and [REDACTED]. "Happy to help, [REDACTED], if my SIPR account would be convenient. It's on the main address list. We decided [REDACTED] was serious and have sought to help..." The Captain replied to PETRAEUS's email, "Sir, I will be happy to send these on SIPR to your account for [REDACTED]..." Based on my training, experience, and information reviewed to date in this investigation, the email chain related to a document or series of documents provided by PETRAEUS to [REDACTED] which contained classified information. This

¹ SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

email correspondence between [REDACTED] and the Captain reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

23. Between July 13, 2011 and July 15, 2011, [REDACTED] and a U.S. Army Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED], emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED] on July 15, 2011, he advised he was working on the storyboards and asked her for "a good SIPR number." Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) PETRAEUS at email account [REDACTED]. [REDACTED] response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.
24. Based on these facts, there is probable cause to believe that PETRAEUS's email account, [REDACTED], contains substantive communications regarding PETRAEUS's sharing of classified information as well as [REDACTED] access to and retention of classified information.

BACKGROUND CONCERNING EMAIL

25. In my training and experience, I have learned that US CENTCOM provides electronic mail ("email") access to uniformed and civilian employees. These users are provided an email account for use in their official duties. Consequently, US CENTCOM computers are likely to contain stored electronic communications (including retrieved and unretrieved email for US CENTCOM users) and information concerning users and their use of US CENTCOM services. This information would include details regarding users of US CENTCOM service, such as the user's full name, physical locations, telephone numbers and other identifiers, account access information, email transaction information, and alternative email addresses. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
26. In general, an email that is sent to a CENTCOM subscriber is stored in the subscriber's "mail box" on CENTCOM servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on CENTCOM servers indefinitely.
27. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to CENTCOM servers, and then transmitted to its end destination. CENTCOM often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the CENTCOM server, the email can remain on the system indefinitely.
28. A CENTCOM subscriber can also store files, including emails, files and other data, on servers maintained and/or owned by CENTCOM.

29. Subscribers to CENTCOM might not store, on their home computers, copies of the emails stored in their CENTCOM account. This is particularly true when the subscriber accesses their CENTCOM account through the web, or if they do not maintain particular emails or files in their residence or on their home computer.

30. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

31. In my training and experience, in some cases email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. Such information may

constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

LOCATION TO BE SEARCHED

32. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the requested warrant to require US CENTCOM to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Attachment A, the information described in Attachment B will be subject to seizure by law enforcement.
33. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information associated with a certain account, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by US CENTCOM, headquartered at MacDill Air Force Base, Tampa, Florida, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

CONCLUSION

34. Based on my training and experience, and the facts as set forth in this affidavit, your affiant asserts there is probable cause to believe that stored in the email account,

[REDACTED], there exists evidence of a crime relating to:

(a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

35. Based on the foregoing, I request that the Court issue the requested search warrant.

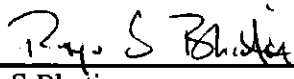
Because the warrant will be served on US CENTCOM, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

36. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by Title 18, United States Code, Section 2711; and Title 18, United States Code, Sections 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is “a district court of the United States that has jurisdiction over the offenses being investigated,” Title 18, United States Code, Sections 1924, 793(e), and 371. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

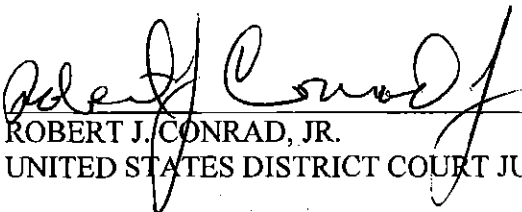
37. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Respectfully submitted,



Raju S Bhatia
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this, the 8th day of August, 2013.




ROBERT J. CONRAD, JR.
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A

Particular Account To Be Searched

This warrant applies to records and other information (including the contents of communications) for the account associated with the email address

 that is stored at premises controlled by US Central Command, which accepts service of legal process at MacDill Air Force Base, Tampa, Florida.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed by CENTCOM ("the Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the account listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, and log files;
- c. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- d. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information To Be Seized by the Government

1. All records or information described above in Section I that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant, including, for the account identified on Attachment A:
 - a. All records or information related to any communications between PETRAEUS and [REDACTED];
 - b. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;
 - c. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
 - d. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided by PETRAEUS to [REDACTED];
 - e. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
 - f. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;
 - g. All records or information related to any communications from June 2012 to the present between PETRAEUS and any other person concerning ongoing law enforcement investigations;

- h. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS or [REDACTED];
 - i. Any information recording PETRAEUS's or [REDACTED] schedule or travel from December 2008 to the present;
and
 - j. Records evidencing the use of the Internet, including records of Internet Protocol addresses used;
- 2. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.
- 3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

MyBook Essential hard drive serial: WCAV5L400801T,
and contents, as described in Affidavit and Attachments
incorporated herein.

)
)
) Case No. 3:13mj 277
)
)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of North Carolina
(Identify the person or describe the property to be searched and give its location):
See Attachment A which is incorporated fully herein

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property to be seized):
See Attachment B which is incorporated fully herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before October 4, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for days (not to exceed 30).

☐ until, the facts justifying, the later specific date of .

Date and time issued:

Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)MyBook Essential hard drive, serial WCAV5L400801T as
described in Affidavit and Attachments, incorporated fully
herein.

Case No. 3:13mj 277

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A, which is incorporated fully herein.

located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See attachment B which is incorporated fully herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. 1924
 18 U.S.C. 793(e)

Offense Description
 Unauthorized removal and retention of classified documents and materials.
 Unauthorized possession, communication and willful retention of national defense information

The application is based on these facts:

See attached Affidavit which is incorporated fully herein

☒ Continued on the attached sheet.

Certified to be a true and correct copy of the original. Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

U.S. District Court

Frank G. Johns, Clerk

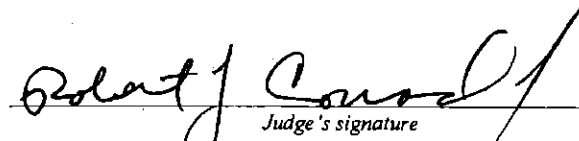
Western District of N.C.

By: 
Deputy ClerkDate: 09/20/2013 Sworn to before me and signed in my presence.Date: 09/20/2013City and state: Charlotte, North Carolina

Applicant's signature

Diane Wehner, Special Agent, FBI

Printed name and title



Judge's signature

Robert J. Conrad, Jr., United States District Court Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Diane M. Wehner, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for electronic information associated with certain hard drives supplied by the National Defense University (NDU)¹. The information to be searched is described in the following paragraphs and in Attachment A, all incorporated fully by reference herein.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for over 7 years. I have investigated matters involving complex financial fraud, public corruption and counterterrorism. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by individuals attempting to conceal their illegal behavior. I have also received specialized training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

¹ NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.
5. For the reasons set forth below, there is probable cause to believe that the electronic records held on the following hard drives: a My Book Essential hard drive, serial: WCAV5L25257IT, a My Book Essential hard drive, serial: WCAZA5221633 and a My Book Essential hard drive, serial: WCAV5L400801T (all described in detail in Attachment A) contain evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful communication and/or retention of classified information.
6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.

9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."

10. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

11. PETRAEUS is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about July 4, 2010 to July 18, 2011, PETRAEUS served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, PETRAEUS served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, PETRAEUS held a United States government security clearance allowing him access to classified United States government information. According to a Department of Defense (DOD) official, to obtain that clearance, PETRAEUS was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
12. [REDACTED] is a researcher and author of a biography of PETRAEUS, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. According to a DOD official, to obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled

to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

13. In 2012, [REDACTED] was the subject of an FBI Tampa Division (FBI Tampa) computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1. This complaint alleged the receipt of threatening and harassing emails from an unknown individual. Witness 1 claimed to have friendships with several high-ranking public and military officials.
14. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of PETRAEUS, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified PETRAEUS's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that PETRAEUS personally requested that Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that PETRAEUS believed the alleged cyber stalker possessed information which could "embarrass" PETRAEUS and other public officials. Ultimately the FBI determined, based upon the investigation, that [REDACTED] was the individual who had sent the emails to Witness 1.
15. On September 24, 2012 as part of the FBI Tampa investigation, [REDACTED] consented to a search of two laptops and two external hard drives belonging to her. A review of the digital media contained on these devices revealed over 100 items which

were identified by Charlotte Computer Analysis Response Team (CART) Forensic Examiners as potentially containing classified information, up to the Secret level.

16. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with [REDACTED]. He denied providing any classified documents to [REDACTED] or having any arrangement to provide her with classified information. PETRAEUS stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.

17. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from PETRAEUS.

18. During interviews conducted of [REDACTED] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of email accounts using non-attributable names and pre-paid cellular telephones. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if all the accounts were identified because both [REDACTED] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [REDACTED] September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

19. On November 12, 2012, Agents from the Charlotte and Tampa Divisions of the FBI participated in a consensual search of [REDACTED] residence in [REDACTED], North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital media as well as four boxes and one folder of documents. On this same date, [REDACTED] administrative assistant voluntarily provided the FBI with digital media as well as one box of documents which she maintained in her home in relation to her employment with [REDACTED]. A review of the seized materials has identified to date hundreds of potentially classified documents, including more than 300 marked Secret, on digital images maintained on various pieces of electronic media.

20. Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. [REDACTED] traveled into and out of

Afghanistan several times between September 2010 and July 2011 to conduct research for a biography on PETRAEUS. During this time, PETRAEUS was serving as the International Security Assistance Force (ISAF) Commander.

21. [REDACTED] paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting [REDACTED], access to classified information for the purpose of writing his biography.

A. Communications Regarding Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED] sent an email to PETRAEUS at email account

[REDACTED] The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, your affiant believes the email related to a document or series of documents provided by PETRAEUS to [REDACTED] which contained classified information.

23. Between July 13, 2011 and July 15, 2011, [REDACTED] and a U.S. Army Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED], emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED] on July 15, 2011, he advised he was

working on the storyboards and asked her for "a good SIPR number."² Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) PETRAEUS at email account [REDACTED]. [REDACTED] response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel likely reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

24. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED], and PETRAEUS, using email address [REDACTED], discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which PETRAEUS addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing PETRAEUS's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

² SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED]"

[REDACTED] the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there." In response PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address

[REDACTED], and [REDACTED], using email address

[REDACTED] exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED].

PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about PETRAEUS's willingness to share the files writing: "[I]'ll protect them. And I'll protect you."

PETRAEUS later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."³ PETRAEUS continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!**" (emphasis added).

³ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

27. Your affiant believes that PETRAEUS's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified.

28. Your affiant believes PETRAEUS and [REDACTED] communicated about the sharing of classified information via PETRAEUS's NIPR⁴ email account. Additionally, based on paragraph 23 above, your affiant believes PETRAEUS allowed classified documents for [REDACTED] to be sent to his SIPR email account.

BACKGROUND CONCERNING NDU COLLECTION

29. Through my training and experience, I have learned that in accordance with the provisions of Title 44, United States Code, Section 3301, 1, PETRAEUS transferred and delivered to NDU, for inclusion in the collections of NDU's library, a collection of personal papers and other non-record personal property.

30. In general, the collection is made up of PETRAEUS's personal files. The collection includes both classified and unclassified documents. The classified collection contains items such as reports, briefings, background material and glossaries. The unclassified collection includes items such as speeches, talking points to the press, newspaper articles and photographs.

31. PETRAEUS's physical documents were provided to NDU in September 2011.

PETRAEUS's electronic documents were provided to NDU in May or June 2012 via hard drives.

32. PETRAEUS's historian provided NDU with three hard drives related to PETRAEUS; two classified and one unclassified. The historian provided two classified hard drives as

⁴ NIPR is an acronym for Non-Classified Internet Protocol Router network, a U.S. government communication system allowing for the exchange of sensitive but unclassified information.

one hard drive contained NATO classified information and the other hard drive contained United States classified information. Later, PETRAEUS's historian wanted to add additional information to the single unclassified hard drive, therefore, PETRAEUS's historian asked NDU to return it. PETRAEUS's historian then combined all the unclassified information onto a single hard drive that was provided to NDU. Both the unclassified hard drive and classified hard drives contain information related to PETRAEUS's career, including his time as Commander of the International Security Assistance Force.

33. The unclassified hard drive contained photographs, speeches made by PETRAEUS, newspaper articles, talking points to the press, administrative paperwork, including tracking calendars and orders, as well as PETRAEUS's NIPR email.
34. The classified hard drives primarily contain PETRAEUS's SIPR email, as well as briefings, classified talking points, reference material, background briefs, maps and daily updates.
35. On or about August 6, 2013, NDU consented to a search of two hard drives from PETRAEUS's collection. A My Book Essential hard drive, serial: WCAV5L25257IT and a My Book Essential hard drive, serial: WCAZA5221633 were transferred from a NDU representative to FBI Agents from the Washington Field Office. The hard drives were then shipped to FBI Charlotte and are currently in the possession of FBI Charlotte. The hard drives are maintained by FBI employees not assigned to the instant matter.
36. On or about August 22, 2013, NDU consented to a search of a My Book Essential hard drive, serial: WCAV5L400801T. This hard drive had been inadvertently overlooked when NDU provided consent on the other two hard drives on or about August 6, 2013.

37. Because it is probable that these drives contain email communications through Petraeus's retirement from the military, there is probable cause to believe they contain communications between Petraeus and [REDACTED], including an email sent to Petraeus's SIPR account attaching a classified document intended for delivery to [REDACTED].

LOCATION TO BE SEARCHED

38. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the requested warrant to require FBI Charlotte to disclose to the government the contents of the hard drives described herein (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Attachment A, the information described in Attachment B will be subject to seizure by law enforcement.

39. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information found on certain hard drives, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by FBI Charlotte, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, *inter alia*, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

CONCLUSION

40. Based upon the foregoing, your affiant submits that there is sufficient probable cause to believe that stored on the hard drives, there exists evidence of a crime relating to: a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

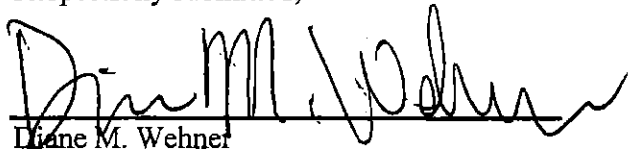
41. Based on the foregoing, I request that the Court issue the requested search warrant.

Because the warrant will be served on FBI Charlotte, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

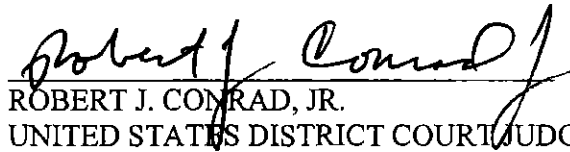
42. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Respectfully submitted,



Diane M. Wehner
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this, the 20th day of September, 2013.


ROBERT J. CONRAD, JR.
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A

Particular Account To Be Searched

This warrant applies to records and other information (including the contents of communications) contained on the My Book Essential hard drive, serial: WCAV5L25257IT, the My Book Essential hard drive, serial: WCAZA5221633 and the MyBook Essential hard drive, serial WCAV5L400801T that are stored at premises controlled by the FBI, which accepts service of legal process at FBI Charlotte, Charlotte, North Carolina.

ATTACHMENT B

Particular Things To Be Seized

1. All records, information, documents and items on the hard drives that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant:
 - a. All records or information related to any communications between PETRAEUS and [REDACTED]
 - b. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;
 - c. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
 - d. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided by PETRAEUS to [REDACTED];
 - e. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
 - f. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

- g. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS;
 - h. Any information recording PETRAEUS's schedule or travel from December 2008 to the present;
- 2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

MyBook Essential hard drive serial: WCAV5L252571T,
and contents, as described in Affidavit and Attachments
incorporated herein.

Case No.

3:13mj-278

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of North Carolina
(identify the person or describe the property to be searched and give its location):
See Attachment A which is incorporated fully herein

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):
See Attachment B which is incorporated fully herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before October 4, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m.

☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: _____

Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature_____
Printed name and title

UNITED STATES DISTRICT COURT

for the
Western District of North CarolinaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)MyBook Essential hard drive, serial WCAV5L252571T as
described in Affidavit and Attachments, incorporated fully
herein.

Case No. 3:13mj278

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A, which is incorporated fully herein.

located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See attachment B which is incorporated fully herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. 1924

18 U.S.C. 793(e)

Offense Description

Unauthorized removal and retention of classified documents and materials.

Unauthorized possession, communication and willful retention of national defense information

The application is based on these facts:

See attached Affidavit which is incorporated fully herein

☒ Continued on the attached sheet.

Certified to be a true and correct copy of the original. Notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

U.S. District Court

Frank G. Johns, Clerk

Western District of N.C.

By: Cynthia Hilly
Deputy Clerk

Date: 09/23/2013 Sworn to before me and signed in my presence.

Date: 09/20/2013

City and state: Charlotte, North Carolina

Diane M. Wehner
Applicant's signature

Diane Wehner, Special Agent, FBI

Printed name and title

Robert J. Conrad Jr.
Judge's signature

Robert J. Conrad Jr., United States District Court Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Diane M. Wehner, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for electronic information associated with certain hard drives supplied by the National Defense University (NDU)¹. The information to be searched is described in the following paragraphs and in Attachment A, all incorporated fully by reference herein.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for over 7 years. I have investigated matters involving complex financial fraud, public corruption and counterterrorism. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by individuals attempting to conceal their illegal behavior. I have also received specialized training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

¹ NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.
5. For the reasons set forth below, there is probable cause to believe that the electronic records held on the following hard drives: a My Book Essential hard drive, serial: WCAV5L25257IT, a My Book Essential hard drive, serial: WCAZA5221633 and a My Book Essential hard drive, serial: WCAV5L400801T (all described in detail in Attachment A) contain evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful communication and/or retention of classified information.
6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.
9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."

10. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

11. PETRAEUS is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about July 4, 2010 to July 18, 2011, PETRAEUS served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, PETRAEUS served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, PETRAEUS held a United States government security clearance allowing him access to classified United States government information. According to a Department of Defense (DOD) official, to obtain that clearance, PETRAEUS was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
12. [REDACTED] is a researcher and author of a biography of PETRAEUS, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. According to a DOD official, to obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled

to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

13. In 2012, [REDACTED] was the subject of an FBI Tampa Division (FBI Tampa) computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1. This complaint alleged the receipt of threatening and harassing emails from an unknown individual. Witness 1 claimed to have friendships with several high-ranking public and military officials.
14. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of PETRAEUS, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified PETRAEUS's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that PETRAEUS personally requested that Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that PETRAEUS believed the alleged cyber stalker possessed information which could "embarrass" PETRAEUS and other public officials. Ultimately the FBI determined, based upon the investigation, that [REDACTED] was the individual who had sent the emails to Witness 1.
15. On September 24, 2012 as part of the FBI Tampa investigation, [REDACTED] consented to a search of two laptops and two external hard drives belonging to her. A review of the digital media contained on these devices revealed over 100 items which

were identified by Charlotte Computer Analysis Response Team (CART) Forensic Examiners as potentially containing classified information, up to the Secret level.

16. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with [REDACTED]. He denied providing any classified documents to [REDACTED] or having any arrangement to provide her with classified information. PETRAEUS stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.

17. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from PETRAEUS.

18. During interviews conducted of [REDACTED] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of email accounts using non-attributable names and pre-paid cellular telephones. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if all the accounts were identified because both [REDACTED] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [REDACTED]'s September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

19. On November 12, 2012, Agents from the [REDACTED] and Tampa Divisions of the FBI participated in a consensual search of [REDACTED]'s residence in Charlotte, North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital media as well as four boxes and one folder of documents. On this same date, [REDACTED]'s administrative assistant voluntarily provided the FBI with digital media as well as one box of documents which she maintained in her home in relation to her employment with [REDACTED]. A review of the seized materials has identified to date hundreds of potentially classified documents, including more than 300 marked Secret, on digital images maintained on various pieces of electronic media.

20. Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. [REDACTED] traveled into and out of

Afghanistan several times between September 2010 and July 2011 to conduct research for a biography on PETRAEUS. During this time, PETRAEUS was serving as the International Security Assistance Force (ISAF) Commander.

21. [REDACTED]'s paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting [REDACTED] access to classified information for the purpose of writing his biography.

A. Communications Regarding Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED], sent an email to PETRAEUS at email account [REDACTED]. The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, your affiant believes the email related to a document or series of documents provided by PETRAEUS to [REDACTED], which contained classified information.
23. Between July 13, 2011 and July 15, 2011, [REDACTED] and a U.S. Army Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED] emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED] on July 15, 2011, he advised he was

working on the storyboards and asked her for "a good SIPR number."² Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) PETRAEUS at email account [REDACTED]. [REDACTED] response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel likely reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

24. From June 12, 2011 through June 15, 2011, [REDACTED] using email address [REDACTED] and PETRAEUS, using email address [REDACTED] discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which PETRAEUS addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing PETRAEUS's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED] email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

² SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED]
[REDACTED], the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there." In response PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address [REDACTED] and [REDACTED], using email address [REDACTED] exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED]. PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about PETRAEUS's willingness to share the files writing: "[I]'ll protect them. And I'll protect you." PETRAEUS later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."³ PETRAEUS continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!**" (emphasis added).

³ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

27. Your affiant believes that PETRAEUS's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED] --- are classified.

28. Your affiant believes PETRAEUS and [REDACTED] communicated about the sharing of classified information via PETRAEUS's NIPR⁴ email account. Additionally, based on paragraph 23 above, your affiant believes PETRAEUS allowed classified documents for [REDACTED] to be sent to his SIPR email account.

BACKGROUND CONCERNING NDU COLLECTION

29. Through my training and experience, I have learned that in accordance with the provisions of Title 44, United States Code, Section 3301, 1, PETRAEUS transferred and delivered to NDU, for inclusion in the collections of NDU's library, a collection of personal papers and other non-record personal property.

30. In general, the collection is made up of PETRAEUS's personal files. The collection includes both classified and unclassified documents. The classified collection contains items such as reports, briefings, background material and glossaries. The unclassified collection includes items such as speeches, talking points to the press, newspaper articles and photographs.

31. PETRAEUS's physical documents were provided to NDU in September 2011. PETRAEUS's electronic documents were provided to NDU in May or June 2012 via hard drives.

32. PETRAEUS's historian provided NDU with three hard drives related to PETRAEUS; two classified and one unclassified. The historian provided two classified hard drives as

⁴NIPR is an acronym for Non-Classified Internet Protocol Router network, a U.S. government communication system allowing for the exchange of sensitive but unclassified information.

one hard drive contained NATO classified information and the other hard drive contained United States classified information. Later, PETRAEUS's historian wanted to add additional information to the single unclassified hard drive, therefore, PETRAEUS's historian asked NDU to return it. PETRAEUS's historian then combined all the unclassified information onto a single hard drive that was provided to NDU. Both the unclassified hard drive and classified hard drives contain information related to PETRAEUS's career, including his time as Commander of the International Security Assistance Force.

33. The unclassified hard drive contained photographs, speeches made by PETRAEUS, newspaper articles, talking points to the press, administrative paperwork, including tracking calendars and orders, as well as PETRAEUS's NIPR email.
34. The classified hard drives primarily contain PETRAEUS's SIPR email, as well as briefings, classified talking points, reference material, background briefs, maps and daily updates.
35. On or about August 6, 2013, NDU consented to a search of two hard drives from PETRAEUS's collection. A My Book Essential hard drive, serial: WCAV5L25257IT and a My Book Essential hard drive, serial: WCAZA5221633 were transferred from a NDU representative to FBI Agents from the Washington Field Office. The hard drives were then shipped to FBI Charlotte and are currently in the possession of FBI Charlotte. The hard drives are maintained by FBI employees not assigned to the instant matter.
36. On or about August 22, 2013, NDU consented to a search of a My Book Essential hard drive, serial: WCAV5L400801T. This hard drive had been inadvertently overlooked when NDU provided consent on the other two hard drives on or about August 6, 2013.

37. Because it is probable that these drives contain email communications through Petraeus's retirement from the military, there is probable cause to believe they contain communications between Petraeus and [REDACTED], including an email sent to Petraeus's SIPR account attaching a classified document intended for delivery to [REDACTED]

LOCATION TO BE SEARCHED

38. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the requested warrant to require FBI Charlotte to disclose to the government the contents of the hard drives described herein (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Attachment A, the information described in Attachment B will be subject to seizure by law enforcement.

39. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information found on certain hard drives, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by FBI Charlotte, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

CONCLUSION

40. Based upon the foregoing, your affiant submits that there is sufficient probable cause to believe that stored on the hard drives, there exists evidence of a crime relating to: a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

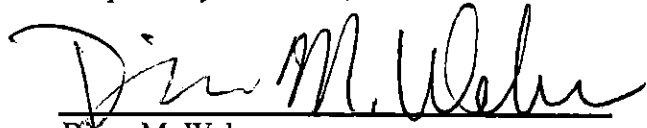
41. Based on the foregoing, I request that the Court issue the requested search warrant.

Because the warrant will be served on FBI Charlotte, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING


42. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Respectfully submitted,



Diane M. Wehner
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this, the 20th day of September, 2013.


ROBERT J. CONRAD, JR.
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A

Particular Account To Be Searched

This warrant applies to records and other information (including the contents of communications) contained on the My Book Essential hard drive, serial: WCAV5L25257IT, the My Book Essential hard drive, serial: WCAZA5221633 and the MyBook Essential hard drive, serial WCAV5L400801T that are stored at premises controlled by the FBI, which accepts service of legal process at FBI Charlotte, Charlotte, North Carolina.

ATTACHMENT B

Particular Things To Be Seized

1. All records, information, documents and items on the hard drives that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant:
 - a. All records or information related to any communications between PETRAEUS and [REDACTED];
 - b. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;
 - c. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
 - d. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided by PETRAEUS to [REDACTED];
 - e. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
 - f. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

- g. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS;
 - h. Any information recording PETRAEUS's schedule or travel from December 2008 to the present;
- 2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT

for the
Western District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

MyBook Essential hard drive serial: WCAZA5221633,
and contents, as described in Affidavit and Attachments
incorporated herein.

)
)
) Case No. 3:13mj 279
)
)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of North Carolina
(Identify the person or describe the property to be searched and give its location):
See Attachment A which is incorporated fully herein

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the
property to be seized):
See Attachment B which is incorporated fully herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before October 4, 2013

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been
established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Robert J. Conrad, Jr.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: _____

Judge's signature

City and state: Charlotte, North Carolina

Robert J. Conrad, U.S. District Court Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the
Western District of North CarolinaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)MyBook Essential hard drive, serial WCAZA5221633 as
described in Affidavit and Attachments, incorporated fully
herein.

Case No.

3:13mj 279

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A, which is incorporated fully herein.

located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See attachment B which is incorporated fully herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. 1924.

18 U.S.C. 793(e)

Offense Description

Unauthorized removal and retention of classified documents and materials.

Unauthorized possession, communication and willful retention of national defense information

The application is based on these facts:

See attached Affidavit which is incorporated fully herein

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested

Certified to be a true and correct copy of the original. U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

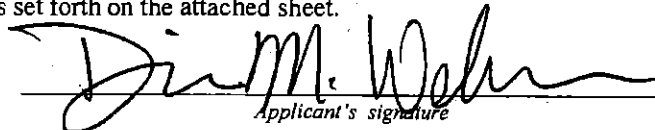
U.S. District Court

Frank G. Johns, Clerk

Western District of N.C.

By: 

Sworn to before me and signed in my presence.

Date: 9/23/2013Date: 09/20/2013City and state: Charlotte, North Carolina

Applicant's signature

Diane Wehner, Special Agent, FBI

Printed name and title



Judge's signature

Robert J. Conrad, Jr., United States District Court Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Diane M. Wehner, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for electronic information associated with certain hard drives supplied by the National Defense University (NDU)¹. The information to be searched is described in the following paragraphs and in Attachment A, all incorporated fully by reference herein.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed as such for over 7 years. I have investigated matters involving complex financial fraud, public corruption and counterterrorism. I am currently assigned to the Charlotte, North Carolina FBI office. Through investigations, experience, and training, I have become familiar with methods and operations employed by individuals attempting to conceal their illegal behavior. I have also received specialized training in the proper collection, retention, and dissemination of classified information.
3. The facts in this affidavit come from my personal observations, my training and experience, evidentiary review, and information obtained from other Agents, government officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

¹NDU is an acronym for National Defense University. NDU is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is located on the grounds of Fort Lesley McNair in Washington, D.C.

STATUTORY AUTHORITY

4. The FBI has been conducting an investigation of DAVID PETRAEUS and [REDACTED] [REDACTED] for possible violations of: (a) unauthorized removal and retention of classified documents and material, in violation of Title 18, United States Code, Section 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of Title 18, United States Code, Section 371.
5. For the reasons set forth below, there is probable cause to believe that the electronic records held on the following hard drives: a My Book Essential hard drive, serial: WCAV5L25257IT, a My Book Essential hard drive, serial: WCAZA5221633 and a My Book Essential hard drive, serial: WCAV5L400801T (all described in detail in Attachment A) contain evidence, fruits, and/or instrumentalities of violations of federal law, including, inter alia, the unlawful communication and/or retention of classified information.
6. Title 18, United States Code, Section 1924(a) states:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

18 U.S.C. § 1924(a).

7. Title 18, United States Code, Section 793(e) states:

Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(e).

8. Title 18, United States Code, Section 371, makes punishable, by up to five years in prison, a conspiracy among two or more persons to commit any offense against the United States.
9. Classified information is defined by Executive Order 13526 (E.O. 13526) and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in the E.O. 13526; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."

10. Pursuant to E.O. 13526, a person may only gain access to classified information if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a need-to-know the information.

PROBABLE CAUSE

11. PETRAEUS is a retired United States Army General. From on or about October 31, 2008 to June 30, 2010, PETRAEUS served as Commander of the United States Central Command. From on or about July 4, 2010 to July 18, 2011, PETRAEUS served as Commander of the International Security Assistance Force. From on or about September 6, 2011 to November 9, 2012, PETRAEUS served as Director of the Central Intelligence Agency (CIA). At all times relevant to this affidavit, PETRAEUS held a United States government security clearance allowing him access to classified United States government information. According to a Department of Defense (DOD) official, to obtain that clearance, PETRAEUS was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.
12. [REDACTED] is a researcher and author of a biography of PETRAEUS, published in January 2012. From on or about July 18, 2003 until on or about November 14, 2012, [REDACTED] held a United States government security clearance allowing her access to classified United States government information. According to a DOD official, to obtain that clearance, [REDACTED] was required to and would have agreed to properly protect classified information by not disclosing such information to persons not entitled

to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations.

13. In 2012, [REDACTED] was the subject of an FBI Tampa Division (FBI Tampa) computer intrusion investigation concerning alleged cyber stalking activity. This investigation was predicated on a complaint received from Witness 1. This complaint alleged the receipt of threatening and harassing emails from an unknown individual. Witness 1 claimed to have friendships with several high-ranking public and military officials.
14. Evidence gathered during the FBI Tampa investigation indicated that someone had access to the personal schedule of PETRAEUS, who was then the Director of the CIA. This access indicated a potential breach of security. On or about June 22, 2012, FBI Headquarters (FBIHQ) notified PETRAEUS's security detail of the ongoing computer intrusion investigation and the potential security issue. On July 19, 2012, FBI Tampa was notified by Witness 1 that he/she no longer wished to press charges against the cyber stalker. On August 10, 2012, Witness 1 informed FBI Tampa that PETRAEUS personally requested that Witness 1 withdraw his/her complaint and "call off the G-men." On August 13, 2012, Witness 1 advised FBI Tampa that PETRAEUS believed the alleged cyber stalker possessed information which could "embarrass" PETRAEUS and other public officials. Ultimately the FBI determined, based upon the investigation, that [REDACTED] was the individual who had sent the emails to Witness 1.
15. On September 24, 2012 as part of the FBI Tampa investigation, [REDACTED] consented to a search of two laptops and two external hard drives belonging to her. A review of the digital media contained on these devices revealed over 100 items which

were identified by Charlotte Computer Analysis Response Team (CART) Forensic Examiners as potentially containing classified information, up to the Secret level.

16. On October 26, 2012, PETRAEUS was interviewed at CIA Headquarters. PETRAEUS stated that he had had an extramarital affair with [REDACTED]. He denied providing any classified documents to [REDACTED], or having any arrangement to provide her with classified information. PETRAEUS stated that [REDACTED] may have obtained documents in the course of conducting research for a book she was writing. He explained that reporters in theater (Afghanistan), such as [REDACTED], were sometimes granted "off-the-record" access to classified presentations, such as the COMISAF's (Commander, International Security Assistance Force) daily briefings.

17. On November 2, 2012, FBI Tampa interviewed [REDACTED] in Charlotte, North Carolina regarding the potentially classified documents found on her computers. She claimed she came into possession of several of the documents when she was in Afghanistan researching her book about PETRAEUS; however, she was unable to provide specifics as to how she obtained them. [REDACTED] stated that during her time in Afghanistan she was given access to several briefings, including at least one briefing at the Secret level. [REDACTED] advised that reporters were often given such access in order to provide them with situational awareness of the war. In order to receive the briefings, [REDACTED] signed an "off-the-record" agreement, which meant she could not write about classified information she observed. She stated she would sometimes obtain a paper copy of the briefings to preserve the information as research for her book. [REDACTED] advised that she never received classified information from PETRAEUS.

18. During interviews conducted of [REDACTED] and PETRAEUS under the aforementioned FBI Tampa investigation, each advised they used covert methods to communicate with each other. These methods included the use of email accounts using non-attributable names and pre-paid cellular telephones. Several of these covert email accounts were identified during the FBI Tampa investigation; however, it is not known if all the accounts were identified because both [REDACTED] and PETRAEUS stated they could not recall all the account names which they created and used to communicate. During [REDACTED]'s September 25, 2012 interview, she advised that she and PETRAEUS would sometimes share the same account, and would save messages to the draft folder instead of sending them via email.

19. On November 12, 2012, Agents from the [REDACTED] and Tampa Divisions of the FBI participated in a consensual search of [REDACTED] residence in Charlotte, North Carolina to recover any evidence related to cyber stalking, a violation of 18 U.S.C. § 2261A, and the unauthorized removal and retention of classified documents, a violation of 18 U.S.C. § 1924. During the search, numerous items were seized to include digital media as well as four boxes and one folder of documents. On this same date, [REDACTED] administrative assistant voluntarily provided the FBI with digital media as well as one box of documents which she maintained in her home in relation to her employment with [REDACTED]. A review of the seized materials has identified to date hundreds of potentially classified documents, including more than 300 marked Secret, on digital images maintained on various pieces of electronic media.

20. Of the potentially classified documents reviewed to date, the majority relate to U.S. military operations conducted in Afghanistan. [REDACTED] traveled into and out of

Afghanistan several times between September 2010 and July 2011 to conduct research for a biography on PETRAEUS. During this time, PETRAEUS was serving as the International Security Assistance Force (ISAF) Commander.

21. [REDACTED]; paper documents, digital data, and audio files indicate PETRAEUS played an integral role in granting [REDACTED] access to classified information for the purpose of writing his biography.

A. Communications Regarding Potential Mishandling of Classified Information

22. On May 12, 2011, [REDACTED], using email account [REDACTED], sent an email to PETRAEUS at email account

[REDACTED] The subject line of the email read: "what part of 4..." and the body of the email read: "is secret? The stuff in parenthesis, or the second sentence?" Based on my training, experience, and information reviewed to date in this investigation, your affiant believes the email related to a document or series of documents provided by PETRAEUS to [REDACTED], which contained classified information.

23. Between July 13, 2011 and July 15, 2011, [REDACTED] and a U.S. Army Lieutenant Colonel exchanged numerous emails. [REDACTED], using email account [REDACTED] emailed the Lieutenant Colonel at his military email account, seeking information about military operations conducted by the Lieutenant Colonel's unit. In requesting this information, [REDACTED] noted that in the past both storyboards and troop narratives had been useful in conveying such facts. In an email from the Lieutenant Colonel to [REDACTED], on July 15, 2011, he advised he was

working on the storyboards and asked her for "a good SIPR number."² Later on July 15, 2011, [REDACTED] replied to the Lieutenant Colonel's email and carbon copied (cc'd) PETRAEUS at email account [REDACTED]. [REDACTED] response included the following: "[I]f you have classified material, GEN Petraeus has been gracious enough to allow me to have you send the storyboards and material to his SIPR account; I'll pick them up as soon as you send the word! I've copied him on this email. If it's unclass, you can use my AKO or this account." This email correspondence between [REDACTED] and the Lieutenant Colonel likely reflects some agreement by PETRAEUS to provide [REDACTED] access to classified information.

24. From June 12, 2011 through June 15, 2011, [REDACTED], using email address [REDACTED] and PETRAEUS, using email address [REDACTED] discussed several topics, to include files maintained by PETRAEUS. In the email string, which contained the subject line "Chapter 2," [REDACTED] raised issues which PETRAEUS addressed by typing in all capital letters within the body of [REDACTED] original emails. In the email string, while discussing PETRAEUS's files, [REDACTED] wrote, "[T]he Galvin letters are naturally very helpful in this regard (I want more of them!!! I know you're holding back...)" In response to this point in [REDACTED]'s email, PETRAEUS wrote: "THEY'RE IN BOXES AND I'LL GET THEM OUT WHEN WE UNPACK AT THE HOUSE IN LATE JULY/AUG."

² SIPR is an acronym for Secure Internet Protocol Router network, a U.S. government communications system allowing the processing, storage, and communication of classified information up to the SECRET level.

25. [REDACTED] responded: "Thanks for your willingness to get out the boxes! [REDACTED]

[REDACTED] the librarian at NDU, has the full collection as well, if it's easier to just gain access to them there." In response PETRAEUS wrote: "SHE DOESN'T HAVE THE FILES I'VE GOT AT HOME; NEVER GAVE THEM TO HER."

26. In an email string initiated on or about June 19, 2011, PETRAEUS, using email address

[REDACTED], and [REDACTED], using email address

[REDACTED] exchanged over ten emails. In the first email, with the subject line "Found the", PETRAEUS discussed locating his "Galvin files" as well as other files and expressed his willingness to share them with [REDACTED]

PETRAEUS wrote: "[G]iven various reassurances from a certain researcher, I will not triage them!" Your Affiant believes the term "triage" refers to the classified contents of the documents. [REDACTED] expressed her excitement about PETRAEUS's willingness to share the files writing: "[I]'ll protect them. And I'll protect you."

PETRAEUS later responded to [REDACTED], writing, "[M]y files at home only go up to about when I took cmd of the 101st, though there may be some MNSTC-I and other ones. Somewhere in 2003, I stopped nice filing and just started chunking stuff in boxes that gradually have gone, or will go, to NDU. Can search them at some point if they're upstairs, but they're not organized enough at this point..."³ PETRAEUS continued, writing, "[A]nd I think MNSTC-I files went to NDU, though I'm not sure. The key to find there would be the weekly reports that the CIG did with me. Not sure if [REDACTED] kept copies. **Class'd, but I guess I might share!**" (emphasis added).

³ MNSTC-I is an acronym for Multi-National Security Transition Command-Iraq. MNSTC-I was a branch of the Multi-National Force-Iraq (MNF-I). Petraeus was the former commander of MNF-I.

27. Your affiant believes that PETRAEUS's reference to "Class'd" means the documents he is discussing --- and which he indicates he is willing to provide to [REDACTED], --- are classified.

28. Your affiant believes PETRAEUS and [REDACTED], communicated about the sharing of classified information via PETRAEUS's NIPR⁴ email account. Additionally, based on paragraph 23 above, your affiant believes PETRAEUS allowed classified documents for [REDACTED] to be sent to his SIPR email account.

BACKGROUND CONCERNING NDU COLLECTION

29. Through my training and experience, I have learned that in accordance with the provisions of Title 44, United States Code, Section 3301, 1, PETRAEUS transferred and delivered to NDU, for inclusion in the collections of NDU's library, a collection of personal papers and other non-record personal property.

30. In general, the collection is made up of PETRAEUS's personal files. The collection includes both classified and unclassified documents. The classified collection contains items such as reports, briefings, background material and glossaries. The unclassified collection includes items such as speeches, talking points to the press, newspaper articles and photographs.

31. PETRAEUS's physical documents were provided to NDU in September 2011.

PETRAEUS's electronic documents were provided to NDU in May or June 2012 via hard drives.

32. PETRAEUS's historian provided NDU with three hard drives related to PETRAEUS; two classified and one unclassified. The historian provided two classified hard drives as

⁴ NIPR is an acronym for Non-Classified Internet Protocol Router network, a U.S. government communication system allowing for the exchange of sensitive but unclassified information.

one hard drive contained NATO classified information and the other hard drive contained United States classified information. Later, PETRAEUS's historian wanted to add additional information to the single unclassified hard drive, therefore, PETRAEUS's historian asked NDU to return it. PETRAEUS's historian then combined all the unclassified information onto a single hard drive that was provided to NDU. Both the unclassified hard drive and classified hard drives contain information related to PETRAEUS's career, including his time as Commander of the International Security Assistance Force.

33. The unclassified hard drive contained photographs, speeches made by PETRAEUS, newspaper articles, talking points to the press, administrative paperwork, including tracking calendars and orders, as well as PETRAEUS's NIPR email.
34. The classified hard drives primarily contain PETRAEUS's SIPR email, as well as briefings, classified talking points, reference material, background briefs, maps and daily updates.
35. On or about August 6, 2013, NDU consented to a search of two hard drives from PETRAEUS's collection. A My Book Essential hard drive, serial: WCAV5L25257IT and a My Book Essential hard drive, serial: WCAZA5221633 were transferred from a NDU representative to FBI Agents from the Washington Field Office. The hard drives were then shipped to FBI Charlotte and are currently in the possession of FBI Charlotte. The hard drives are maintained by FBI employees not assigned to the instant matter.
36. On or about August 22, 2013, NDU consented to a search of a My Book Essential hard drive, serial: WCAV5L400801T. This hard drive had been inadvertently overlooked when NDU provided consent on the other two hard drives on or about August 6, 2013.

37. Because it is probable that these drives contain email communications through Petraeus's retirement from the military, there is probable cause to believe they contain communications between Petraeus and [REDACTED] including an email sent to Petraeus's SIPR account attaching a classified document intended for delivery to [REDACTED].

LOCATION TO BE SEARCHED

38. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the requested warrant to require FBI Charlotte to disclose to the government the contents of the hard drives described herein (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Attachment A, the information described in Attachment B will be subject to seizure by law enforcement.

39. Based upon the foregoing, your affiant submits that probable cause exists for the issuance of a search warrant for information found on certain hard drives, as more fully described in Attachment A to this affidavit, stored at premises owned, maintained, controlled, or operated by FBI Charlotte, to search for evidence of: (a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

CONCLUSION

40. Based upon the foregoing, your affiant submits that there is sufficient probable cause to believe that stored on the hard drives, there exists evidence of a crime relating to: a) unauthorized removal and retention of classified documents and material, in violation of 18 U.S.C. § 1924; (b) unauthorized possession and, inter alia, attempted communication and willful communication of national defense information to someone not entitled to receive it, as well as the willful retention of national defense information, in violation of 18 U.S.C. § 793(e); and (c) conspiracy to commit the aforementioned crimes, in violation of 18 U.S.C. § 371.

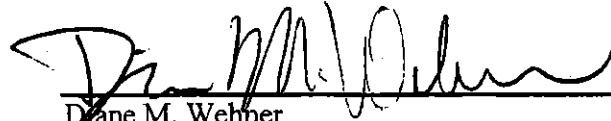
41. Based on the foregoing, I request that the Court issue the requested search warrant.

Because the warrant will be served on FBI Charlotte, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

42. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, it is respectfully requested that the Court issue an order that the search warrant, this affidavit in support of the application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Respectfully submitted,



Diane M. Wehner
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this, the 20th day of September, 2013.



ROBERT J. CONRAD, JR.
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A

Particular Account To Be Searched

This warrant applies to records and other information (including the contents of communications) contained on the My Book Essential hard drive, serial: WCAV5L25257IT, the My Book Essential hard drive, serial: WCAZA5221633 and the MyBook Essential hard drive, serial WCAV5L400801T that are stored at premises controlled by the FBI, which accepts service of legal process at FBI Charlotte, Charlotte, North Carolina.


ATTACHMENT B

Particular Things To Be Seized

1. All records, information, documents and items on the hard drives that constitute fruits, evidence, and instrumentalities of violations of the statutes listed on the warrant:
 - a. All records or information related to any communications between PETRAEUS and [REDACTED];
 - b. All records or information related to any communications, from December 2008 to the present, between PETRAEUS and any other person or entity concerning classified and/or national defense information;
 - c. All records or information, from December 2008 to the present, related to any classified and/or national defense information;
 - d. All records or information, from December 2008 to the present, related to the source(s) or potential source(s) of any classified and/or national defense information provided by PETRAEUS to [REDACTED];
 - e. All records or information, from December 2008 to the present, related to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified and/or national defense information;
 - f. All records or information relating to knowledge of laws, rules, regulations, and/or procedures prohibiting the unauthorized disclosure or retention of classified and/or national defense information;

-
- g. All records or information concerning any email accounts, telephone numbers, or other methods of communication used by PETRAEUS;
 - h. Any information recording PETRAEUS's schedule or travel from December 2008 to the present;
2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

(b)(5); (b)(6); and (b)(7)(C)



From: Savage, David [mailto:David.Savage@latimes.com]

Sent: Monday, November 12, 2012 02:48 PM

To: (b)(6) and (b)(7)(C) (USANCW)

Subject: search warrant

Hi, (b)(6)

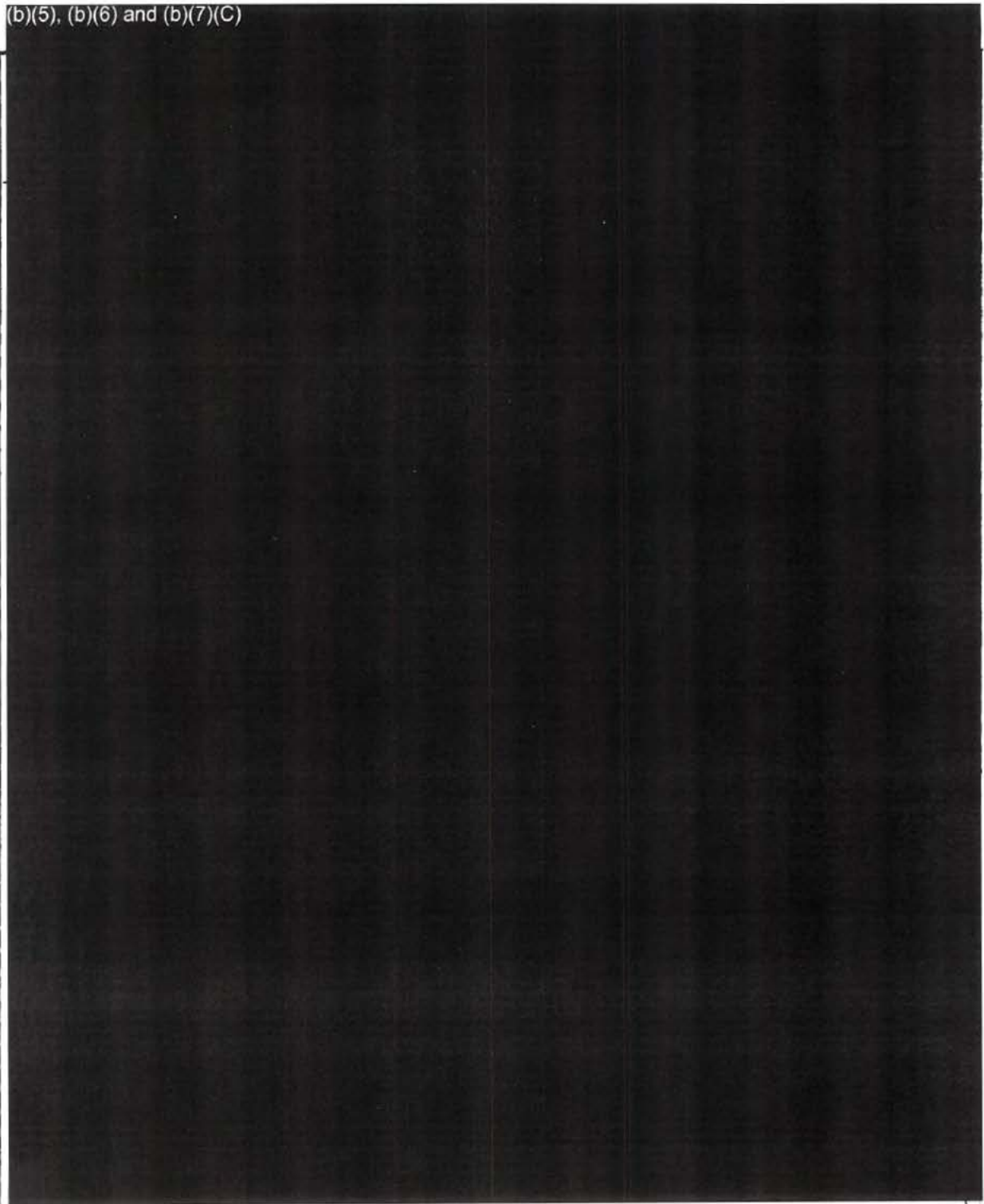
I'm a reporter in Washington for the Tribune papers and was asked to check one point regarding the investigation involving Paula Broadwell and Gen. Petraeus.

Did the FBI file an affidavit in support of a search warrant to examine Broadwell's computer, and if so, can we obtain a copy of the affidavit?

Thanks for any help you can offer,

David Savage
Los Angeles Times/Chicago Tribune
202-824-8337

(b)(5), (b)(6) and (b)(7)(C)



From: Bezdrob, Shayla [mailto:shayla.bezdrob@FOXNEWS.COM]

Sent: Wednesday, July 16, 2014 11:43 AM

To: (b)(6) and (b)(7)(C) (OPA)

Subject: FW: DOJ comment: Petraeus investigation "perplexing and suspicious"

Importance: High

Hi Kevin -

54

I sent this to Brian and wanted to loop you in as well in case you can assist.
Many thanks,
Shayla

Shayla Bezdrob, Producer, Fox News Channel, 400 N Capitol St, NW Suite 550, Washington D.C. 20001
tel: (202) 824-6427 cell [b6]

From: Bezdrob, Shayla
Sent: Wednesday, July 16, 2014 11:32 AM
To: 'Fallon, Brian (OPA)'
Subject: DOJ comment: Petraeus investigation "perplexing and suspicious"
Importance: High

Hi Brian,

We are looking a response/comment from DOJ for a story Catherine Herridge is doing today. Attached is a letter from Re. Chaffetz to AG Holder.

Could you please give us a response to the following:

Rep Chaffetz says he's spoken with or written to AG Holder five times about the Petraeus investigation, but has not yet received an answer. The allegation is that there is a pattern of obstruction.

Could you tell us what your timeframe for a response to Rep. Chaffetz is and what is causing the delay? If AG Holder/DOJ have responded, what is that response?

It has been two years since the investigation in Gen Petraeus has been opened; sources say there is clear evidence that Gen Petraeus had classified documents in his home - why is the investigation still open, what is the delay, given the evidence collected, why is Gen Petraeus not being prosecuted and/or cleared of any wrongdoing if that is indeed the case?

Fox previously reported there was a conflict between the FBI and DOJ over whether to proceed to a prosecution in the case. AG Holder denied knowledge of the conflict, but confirmed in his April testimony, as has FBI Director Comey, that the case remains open.

We would like to include a DOJ response in our reporting today and would appreciate it as soon as possible. Herridge is doing live shots all day.

Many thanks in advance.

Shayla

Shayla Bezdrob, Producer, Fox News Channel, 400 N Capitol St, NW Suite 550, Washington D.C. 20001
tel: (202) 824-6427 cell [b6]

55

To: (b)(6); and (b)(7)(C)
Subject: FW: Seized items to be returned

FYI

From: (b)(6); (USANCW)
Sent: Monday, August 05, 2013 5:22 PM
To: Kendall, David (dkendall@wc.com); Latcovich, Simon (slatcovich@wc.com)
Cc: Scott, (b)(6); (NSD) (JMD); (b)(6); and @usdoj.gov
Subject: Seized items to be returned

David and Simon,

As promised, some of the seized items are being packaged for return to your client.

The following items will be at the FBI Washington Field Office next week:


(b)(6); (b)(7)(C); and (b)(7)(E)




Once the items have been delivered to WFO, we will provide the pick-up details.

Best,

(b)(6);
and (b)



From: (b)(6) USANCW (b)(6) sa.doj.gov	Date: 08/05/2013 17:21:34
To: Kendall, David (DKendall@wc.com) <DKendall@wc.com>, Latcovich, Simon (SLatcovich@wc.com) <S ...	Cc: (b)(6) and (NSD) (JMD) (b)(6) and (b)@usdoj.gov
Folder:	
Subject: Seized items to be returned	
Attachments:	

 Print the page

David and Simon,

As promised, some of the seized items are being packaged for return to your client.

The following items will be at the FBI Washington Field Office next week:

(b)(6); (b)(7)(C); (b)(7)(E)

Once the items have been delivered to WFO, we will provide the pick-up details.

Best,

(b)(6)
and (b)

88

From: (b)(6) (USANCW) (b)(6) <(b)(6)@usa.doj.gov> Date: 04/23/2013 11:03:44
To: (b)(6) and (b) NSD (JMD) (b)(6) and (b)(6)@usdoj.gov Cc:
Folder:
Subject: RE: Our Telephone Conversation This Morning
Attachments:

 Print the page

(b)(5); (b)(6) and (b)(7)(C)

From: (b)(6) and (b)(7) NSD [mailto:(b)(6) and (b)(7)@usdoj.gov]
Sent: Tuesday, April 23, 2013 10:04 AM
To: (b)(6) (USANCW)
Subject: Re: Our Telephone Conversation This Morning

(b)(5); (b)(6) and (b)(7)(C)

From: (b)(6) (USANCW)
Sent: Monday, April 22, 2013 04:05 PM
To: (b)(6) and (b) (NSD)
Subject: FW: Our Telephone Conversation This Morning

(b)(6) and (b)(7)(C)


From: Kendall, David [mailto:DKendall@wc.com]
Sent: Monday, April 22, 2013 11:03 AM
To: (b)(6) (USANCW)
Subject: Our Telephone Conversation This Morning

Dear (b)(6)

It was good to talk to you this morning. As promised, below are the items seized on April 5 which we believe will not be of interest to your investigation, but most of which the General needs now for his various professional and commercial commitments and activities. The numbers correspond to the inventory that the General was provided at the end of the search. Since we (obviously) do not have the items seized, my descriptions of them are to the best of our present knowledge. We understand that you will need to have other agencies, such as the CIA or DOD, check the items generated in those agencies. We would be grateful, however, if you could do whatever you can to facilitate the return of the following, assuming they are not relevant to your investigation:

(b)(6) and (b)(7)(C)

(b)(6) and (b)(7)(C):



Please let me know if you have questions.

I will look forward to hearing from you after your trial about a date we can meet with you in Charlotte, hopefully during the week of May 13. Good luck with your trial.

Best,

David

David E. Kendall
Williams & Connolly LLP
725 Twelfth Street, N.W., Washington, DC 20005
(P) 202-434-5145 | (F) 202-434-5029
dkendall@wc.com | www.wc.com/dkendall

NOTICE:

This message is intended for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by reply or by telephone (call us collect at (202) 434-5000) and immediately delete this message and all its attachments.

Subject: Letter from Senator McCain to Attorney General Holder re Petraeus investigation

Think our last letter on this was to Chaffetz on 9/30/14, indicating that the investigation is ongoing. (b)(5)
(b)(5) but will ask EOUSA to draft a response for OLA sig, in consultation with the Bureau. Please let us know if we should follow another course. Thanks. FB

From: Hall, Stephanie (McCain) [mailto:(b)(6)]
Sent: Tuesday, December 02, 2014 2:01 PM
To: Burton, Faith (OLA)
Subject: Letter from Senator McCain to Attorney General Holder

Dear Faith,

Attached please find a letter from Senator McCain to Attorney General Holder. The hard copy has been placed in the mail. Please let me know if you have any questions or concerns.

Best,
Stephanie

Stephanie Hall
Counsel
Senator John McCain
241 Russell Senate Building
(b)(6)

49

From: Kellner, Kenneth E. (OLA) (JMD) <Kenneth.E.Kellner@usdoj.gov>	Date: 12/02/2014 15:34:09
To: Burton, Faith (OLA) (JMD) <Faith.Burton@usdoj.gov>, (b)(6) (USANCW) (b)(6) usa.doj.gov ...	McKay, Shirley A (OLA) (JMD) Cc: <Shirley.A.McKay@usdoj.gov>, Uriarte, Carlos (ODAG) (JMD) <Car ...
Folder:	
Subject: RE: Letter from Senator McCain to Attorney General Holder re Petraeus investigation	
Attachments: 2014-9-30 CIA David Petraeus - Chaffetz #2891043.pdf	

[Print the page](#)

And here is the letter to Chaffetz.

From: Burton, Faith (OLA)
Sent: Tuesday, December 02, 2014 3:31 PM
To: (b)(6) (USANCW); (b)(6); Kadzik, Peter J (OLA); Wong, Norman (USAE0); Laragy, Scott (USAE0)
Cc: McKay, Shirley A (OLA); Uriarte, Carlos (ODAG); Colborn, Paul P (OLC); Kellner, Kenneth E. (OLA); Hayden, Paul A. (OLA)
Subject: Letter from Senator McCain to Attorney General Holder re Petraeus investigation

Think our last letter on this was to Chaffetz on 9/30/14, indicating that the investigation is ongoing. (b)(5) (b)(5) but will ask EOUSA to draft a response for OLA sig, in consultation with the Bureau. Please let us know if we should follow another course. Thanks. FB

From: Hall, Stephanie (McCain) [mailto:(b)(6)]
Sent: Tuesday, December 02, 2014 2:01 PM
To: Burton, Faith (OLA)
Subject: Letter from Senator McCain to Attorney General Holder

Dear Faith,

Attached please find a letter from Senator McCain to Attorney General Holder. The hard copy has been placed in the mail. Please let me know if you have any questions or concerns.

Best,
Stephanie

Stephanie Hall
Counsel
Senator John McCain
241 Russell Senate Building
(b)(6)

50

**U.S. Department of Justice****Office of Legislative Affairs**

Office of the Assistant Attorney General

Washington, D.C. 20530

SEP 30 2014

The Honorable Jason Chaffetz
U.S. House of Representatives
Washington, DC 20515

Dear Congressman Chaffetz:

This responds to your letter to the Attorney General dated July 15, 2014, which requested information concerning the investigation of former Central Intelligence Agency Director General David Petraeus.

In response to your inquiry, we can advise that the investigation is ongoing. Based on longstanding Department of Justice policy and procedures, we are not in a position to disclose non-public information concerning this pending investigation. This policy serves to protect the integrity of the criminal justice process, including the confidentiality and privacy interests that are important to our law enforcement efforts. While we cannot provide a timeframe for the investigation's conclusion, we can assure you that all decisions will be made in accordance with the *Principles of Federal Prosecution*.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter J. Kadzik".

Peter J. Kadzik
Assistant Attorney General

51

000000

EXPLANATION OF EXEMPTIONS

FOIA: TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by and Executive order to be kept secret in the in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual.
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

PRIVACY ACT: TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to Executive Order 12356 in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability eligibility, or qualification for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his identity would be held in confidence.